DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

19980311 159

DTIC QUALITY INSPECTED 4

DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GIS/LAS/97D-1

A MODEL FOR DETERMINING INFORMATION TO BE CAPTURED REGARDING UNAUTHORIZED COMPUTER ENTRY OF AN AIR FORCE COMPUTER SYSTEM

THESIS

Leslie F. Himebrook
First Lieutenant, USAF

AFIT/GIS/LAS/97D-1

AFIT/GIS/LAS/97D-1

A MODEL FOR
DETERMINING INFORMATION TO BE CAPTURED
REGARDING UNAUTHORIZED COMPUTER ENTRY
OF AN AIR FORCE COMPUTER SYSTEM

THESIS

Presented to the Faculty of the Graduate School of Logistics

and Acquisition Management of the Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the

Requirements for the Degree of

Master of Science in Information Systems Management

Leslie F. Himebrook, B.S.

First Lieutenant, USAF

December 1997

Acknowledgments

As with most of life's endeavors, this thesis could not have been completed without the support of numerous individuals. Without my sponsors, Col. David L. Surlowitz, and Major Byron B. Thatcher, this thesis would have never gotten started. My advisor, Doctor Alan R. Heminger, and my reader, Major Caisson M. Vickery, provided exceptional advice and direction. Without their support, I could not have completed this study. I am also indebted to the superb AFIT library staff, specifically Ms. Patricia A. White, who pointed me in the correct direction for my research endeavors. I am also indebted to Captain Kenneth V. Peifer and Captain Christina M. Anderson, who repeatedly reviewed my drafts and pointed out numerous errors before any drafts were sent to my advisor. Finally, and most importantly, special thanks go to my family and friends. Without their constant support and uplifting, I would have never survived this northern assignment. I would specifically like to thank my parents for their unswerving support, positive encouragement, and for providing the light which guides me. As it says in the second book of Timothy, "...the time has come for my departure. I have fought the good fight, I have finished the race, I have kept the faith."

Les Himebrook

Table of Contents

Page

List of Figures

Figure | Page

Abstract

This thesis presents a model for data for the Air Force to use to capture information about unauthorized attempts to access computer systems. This model takes a management focus, and incorporates the technical focus, intelligence focus, and legal focus as inputs to the management focus. The author used an exploratory, qualitative methodology consisting of an extensive literature review and interviews with experts in the field. These efforts produced the proposed model, which was reviewed by experts in the field using a delphi technique.

The model consists of information that is divided into the following areas:

1. What information was compromised.
2. What type of intrusion occurred.
3. How the intrusion was attempted.
4. Legal issues including the ability to report to law enforcement.
5. Prevention of future intrusions.

This thesis concludes by recommending that:

1. The information should be captured by the individual as close to the intrusion as possible. This is done to increase the accuracy of the information.
2. The information should be passed in a timely and accurate manner to the organization's Computer Emergency Response Team (CERT).
3. The CERT should use the information to attempt to rectify the intrusion.
4. The CERT should aggregate the information in an attempt to evaluate the possibility of an organized intrusion attempt.
5. The CERT should pass relevant information to other system administrators in an attempt to prevent future successful intrusion attempts.

A MODEL FOR

DETERMINING INFORMATION TO BE CAPTURED

REGARDING UNAUTHORIZED COMPUTER ENTRY

OF AN AIR FORCE COMPUTER SYSTEM

I. Introduction

Chapter Overview

> Just as the introduction of orders written on paper a few thousand years ago transformed warfare by expanding a commander's possible campaign and battle moves, so computerization, in its effects on information processing...will create its own revolution in warfighting. (Arquilla, 1994: 25)

In Antiquity, Calimachus of Athens knew the battle plans of King Darius of Persia at the battle of Marathon. Calimachus's knowledge lead him to lengthen his line, weakening his center, knowing that this was where the Persians were strongest. He allowed his center to collapse, and proceeded to use both of his flanks as separate armies, flanking the Persian Army and crushing them from the rear. This use of information allowed the growth of the Helanistic and Roman Cultures, and shaped the history of the western world (Creasy, 1955: 1-2, 19-26). During World War II, the allied forces used disinformation to its advantage. Operation FORTITUDE involved the creation of the fictitious First U.S. Army Group under the command of Lieutenant General Patton in south east England and the fictitious British Fourth Army in Scotland under General Sir Andrew Thorne. These armies succeeded in deceiving Germany into believing that the invasion force of Operation Overlord was bound for Pas de Calais. The delay in Germany determining that the attack in Normandy was primary and not a diversion

allowed the allied forces to obtain a foothold on the continent, and helped lead to the defeat of Germany. This disinformation had significant effects on the history of the past half century (Koch, 1992: 66-77). Since the end of World War II, computers have allowed information, and consequently disinformation, to be accessed more quickly than before. As computers have become linked during the past few decades, this information can be passed more easily from one location to another. It can therefore also be stolen or observed more easily.

The migration of information to computers and the linking of these computers has increased information's accessibility throughout the military enterprise. Unfortunately this same computerization creates new vulnerabilities, because information can be intercepted and/or attacked by adversaries through this computerization. When unfriendly users try to gain access to this computerized information, it is very important to know about this unauthorized access. Therefore steps must be taken to learn about these information attacks. The military has processes in place to obtain some of this information. When attacks are found, information is gathered about the attack. When an attack occurs, an important management decision is: What information is most important to know about attempts to gain unauthorized access? This thesis presents a model for information that the Air Force should capture regarding unauthorized attempts to access Air Force computer systems based on a management perspective and uses a delphi process with experts in the field to improve the model and assess its value.

On a regular basis, the Air Force detects unauthorized access attempts of Air Force information systems. The Air Force has the capability to monitor much of this unauthorized entry into its systems (Thatcher, 1997). In the process of monitoring unauthorized entry, what do we want to know, and therefore what information should the Air Force collect? What information should be collected depends on the purpose.

Among the possible purposes are technical, intelligence, legal, and management. For each of these, different information may be important. For example:

1. Technical Focus
   a. How did someone get into this system?
   b. How can this be prevented from happening again?
2. Intelligence Focus
   a. What value might the information be to an adversary?
   b. What value does the information hold for the Air Force?
3. Legal Focus
   a. Can a legal case be made against the offending party?
4. Management Focus
   a. What are the costs for both a secure and an insecure system?
   b. What can management do to protect information from known threats?
   c. Is the system secure enough?

A manager "shall implement and maintain a program to assure adequate security is provided for all information…" (OMB Circular No. A-130, 1996: 18) and adequate security means "security commensurate with the risk and magnitude of harm resulting from loss, misuse, or unauthorized access to or modification of information" (OMB Circular No. A-130, 1996: 17). This thesis will have a management focus to attempt to address these issues. It will be shown that technical, intelligence, and legal focuses have significant inputs to the management focus. Therefore, this thesis will focus on the question "What information is needed to answer questions regarding unauthorized computer entry."

Background

Ever since knowledge and information have been stored, there have been those who want to steal that information. In the third century BC, Sun Tzu wrote:

> Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant of both your enemy and of yourself, you are certain in every battle to be in peril.
>
> (Sun Tzu, 1963: 11, 84)

The migration of information to computers and networks has increased the information's accessibility, to both friendly and unfriendly users. Since "organizations [have] come to depend on massive, prompt and accurate information flow, the corresponding vulnerabilities inherent in large-scale information systems must be taken into account." (Rona, 1996: 54) Access to computers and networks has added more avenues, both legitimate and unauthorized, to access information. Government studies indicate that the Department of Defense (DoD) "may have been attacked as many as 25,000 times last year [1995]. However, the exact number is not known because...only about 1 in 150 attacks is actually detected and reported" (GAO/AIMD 96-84: 3).

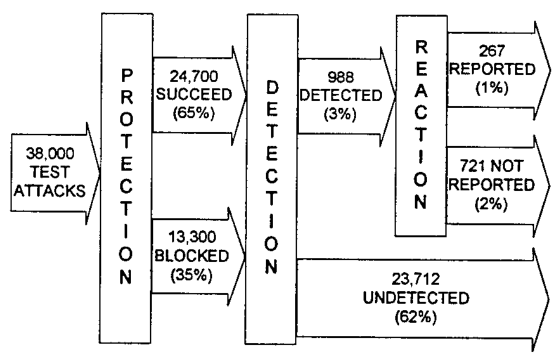

Figure 1. Results of DISA Computer Vulnerability Assessments (1992—1996)

One such study was conducted by the Defense Information Systems Agency (DISA) between 1992 and 1996. In this study, DISA "conducted 38,000 attacks on Defense computer systems to test how well they were protected. DISA successfully

gained access 65 percent of the time (see Figure 1). Of these successful attacks, only 988 or about 3 percent were detected by the target organizations. Of those detected, only 267 attacks or roughly 1 percent was reported to DISA" (GAO/AIMD 96-84: 19-20).

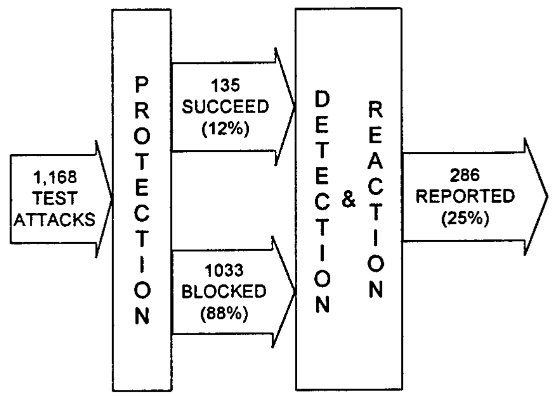

Figure 2. Results of AFCERT Computer Vulnerability Assessment (April 1995)

In similar studies, the Air Force reportedly did better than the DoD average; averaging 12 percent and 25 percent detection and reporting of test break-ins for January and April 1995 respectively (see Figure 2). The information from the Air Force Computer Emergency Response Team (AFCERT) is slightly different from the information obtained from DISA. DISA only reported successful attacks. However, AFCERT reported all detected attacks, regardless of whether or not they were successful (Surlowitz, 1996: 18-20).

The Internet, with over 40 million computers tied together, has become a lucrative target for those individuals who wish to steal or modify information (GAO/AIMD-96-84: 3). With the increased use of the Internet for internal Air Force communication and other critical communication within the DoD, the potential for break-ins becomes even greater.

Every break-in has the potential to do unknown but significant damage to the security of the United States, and at the worst case could cause the loss of American sovereignty. According to Paul Strassmann, distinguished visiting professor at the National Defense University, probably the largest problem is that "...management has washed its hands of [information security], assuming the technicians will take care of it. But it is a management problem, not a technical issue" (Anthes, 1995: 80).

Problem Statement

When knowledge is gained that an individual has unauthorized access to or has attempted to gain unauthorized access to an Air Force computer, what information should a network administrator capture? The managerial focus involves the technical, intelligence, and legal views. This thesis proposes an integrative model that is developed and then is improved by experts using a modified delphi process.

Summary

Data security has become increasingly important in an age of increased computer and network usage. This thesis presents a model for data for the Air Force to capture regarding unauthorized attempts to access computer systems. This model takes a management focus, and incorporates the technical focus, intelligence focus, and legal focus as inputs to the management focus.

II. Background

Chapter Overview

During the literature review, it was found that a majority of the information and research regarding the information that is useful to a manager regarding unauthorized computer entry is divided into three categories. These three areas are technical information, intelligence information, and legal information.

Technical Information

In simple terms, technical information deals with how someone is able to access information. In the past, technical information would have included activities such as breaking into safes and stealing documents. In the age of electronic information storage and exchange, a thief is no longer required to be physically present at the theft site. A thief can break into a system or capture information while it is in transit from one location to another, or even while it is stored.

A computer's access can be divided into one of three areas: from the computer itself, from another computer where the remote computer and the connection is under a manager's control, and from another computer where the remote computer and/or the connections are not under a manager's control (Lou and Armitage, 1996: 13). Every computer is either a stand-alone or is connected to other computers. The following section will discuss the vulnerabilities of stand-alone systems. If the computer is connected to other computers, there are additional vulnerabilities which will be addressed in the following sections. When a computer is connected to other computers, this network may be entirely under a manager's control or may pass through areas that the manager does not control, such as public areas. Finally, this section will discuss the increased vulnerabilities of passing information through public areas, such as using the Internet.

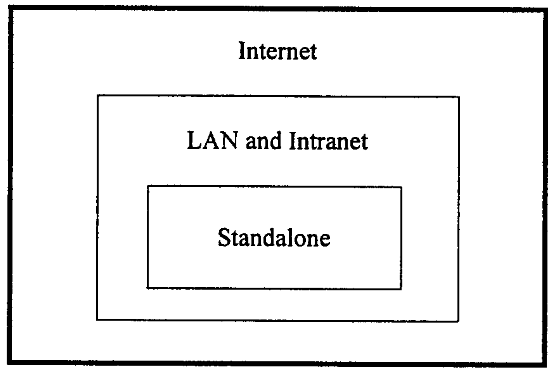

Figure 3. Technical Focus, Levels of Vulnerability of Computerized Information Systems

The Air Force currently intercepts and analyzes information going onto or out of every base, where the base LAN or Intranet connects to the Internet, and stores information which includes typical unauthorized activities. This information is either downloaded daily or in real-time for analysis by the Air Force Computer Emergency Response Team (AFCERT). Those downloaded in real-time are using the latest version of the Automated Security Incident Measurement (ASIM) analysis software. AFCERT is the organization that is responsible for coordinating computer security for the Air Force.

Stand-alone Computer. A stand-alone computer is a computer that is not attached to a network. This is the simplest computer to prevent an intruder from attacking. There are only two ways to attack a stand-alone computer. The first is to be physically present at the computer. Once physically present, information may be copied on to a disk, the entire computer stolen, or the computer may be damaged. Since information may be copied to a disk, stealing a disk with information on it is another form of physical intercept. The second way to attack a stand-alone computer is to be close enough to the computer to intercept electromagnetic emissions from that computer (Schwartau, 1996: 221).

Physical Intercept. If an individual is physically present at a computer, he or she may intercept, interrupt, modify, or fabricate any information on that machine. It is for this reason that unauthorized individuals are kept away by the Security Police, and Air Force personnel can be prosecuted for misuse of government systems and misconduct. Physical security falls back on situations that we can easily understand, such as theft or breaking and entering. It is when information is transferred by non-physical means, that is the focus of this thesis.

Electromagnetic Radiation. Computers, printers, and monitors are all electrical devices that conduct current. Any time that electrical current moves, it creates an electromagnetic signal similar to a transmitter, only with less power. Therefore, it is sometimes possible to intercept this electromagnetic radiation and determine what signals are being processed in an electrical device. The strongest signal from most computer systems is from the monitor, which emits "Van Eck Radiation." Van Eck radiation can be received and used to reconstruct the screen of the monitor which produced that radiation. Van Eck radiation can be intercepted and viewed at distances up to a kilometer away from the monitor. Even if the monitor is turned off, information can still be obtained, though the signal strength will be decreased and therefore the maximum reception distance will also be reduced. This is a vulnerability that must be considered by any system administrator (Schwartau, 1996: 222-224) (Van Eck, 1985: 269-276).

Networked Computers.

Local Area Networks (LANs) and Intranets. A Local Area Network (LAN) and an Intranet are a group of computers that are connected together. Therefore both a LAN and an Intranet have all of the vulnerabilities of a stand-alone computer plus vulnerabilities that exist because of their connections. As information is passed between computers, the information may be compromised as it passes through the links between computers or the information may be intercepted at any computer that it passes through.

A LAN connects computers or other LANs in an organization and passes messages between them using known paths (Fitzgerald and Dennis, 1996: 246-251). An Intranet is similar to a LAN in that is also connects computers in an organization, though it may include multiple sites. Another major difference is that the route a message will take from its origin to its destination is based on the traffic load, length of the message, line quality, etc. In other words, the routing for the message is unknown when it is sent. Since the route is unknown, the vulnerability is unknown, but potentially increased (Fitzgerald and Dennis, 1996: 332-333, 353-356).

Even with the vulnerabilities of a LAN or Intranet system, an intruder must still be physically present, or close enough to capture electromagnetic emissions, in order to be a threat (since by definition all links and computers in a LAN or Intranet are internal to an organization). It is only when information is sent across open lines and such as the Internet that a system can no longer be secured using solely physical protection.

Internet. The Internet, in contrast to LANs and Intranets, sends information through lines and nodes not under the control of a single organization. "The basis for the Internet was [ARPANET], an experiment begun in 1968 by the Defense Department's [Advanced Research Projects Agency] Information Processing Techniques Office (ARPA/IPTO) to connect computers over a network in order to ensure command and control communications in the event of a nuclear war" (Howard, 1997: 8). In the early 1980's, due to the free distribution of the Transmission Control Protocol and Internet Protocol (TCP/IP), the use of ARPANET spread rapidly among universities, research institutes, and businesses. Technology allowed expansion by the simple act of connecting to existing networks. Therefore the ease of connection and the utility of joining led increasing numbers of organizations to join, leading to the Internet as we know it (Luo and Armitage, 1996: 13-14).

While an Intranet and the Internet are very similar in structure, there is one significant difference which causes a huge vulnerability. For both the routing for the message is unknown when it is sent. When a message is sent from one computer to another, the route that the message will take depends on the traffic load, length of the message, line quality, etc. For an Intranet this is not a problem, since all of the nodes in the network are under the organization's control. For the Internet this is not the case. Therefore, the major vulnerability when using the Internet, is that a message will be traveling through nodes that you do not control. At any node not under your control, the message may be intercepted, interrupted, modified, or the address stored for later use in fabricating a message.

The best method to overcome this vulnerability is to use encryption. There are two methods of encryption over the Internet, End-to-End and Link-to-Link. Which method to use is based on where you consider your greatest threat. End-to-End encryption will encrypt the text of a message, and leave the address header in plain text. Therefore, the message can be passed from one node to another with little chance of reading the text of the message. Link-to-Link encryption is more effective against line interception. In this case once a node has decided the next node for the message, it will encrypt the message and send it to the next node. The next node must then decrypt the message before it will know where to forward it, then will re-encrypt it and forward the message. The advantage of this encryption method is that even the header is encrypted. The disadvantage is that it will be in plain text at every node (Braaten and Johannessen, 1992: 264-266). It is also possible to use both End-to-End and Link-to-Link encryption, so that the text of the message is never decrypted between the sending and receiving computers, and the header is encrypted during each link.

Even if the messages are encrypted, there is still a vulnerability. Although an intruder will not be able to decipher the information, he can still gain some information

based on the amount of information passed. Therefore, "dummy" messages may be sent along with the "legitimate" messages in order to maintain a nearly constant rate of information passing (Rackoff and Simon, 1993: 672-675).

Firewalls. A firewall is a collection of software and/or hardware that will prevent (hopefully) an intruder from accessing information within a LAN or Intranet (Fitzgerald and Dennis, 1996: 342-343). A firewall will "protect Internet-attached nets from cyberspace intruders" (Johnson and Tolly, 1995: 62). A good firewall, or series of firewalls, is vital to any system that is attached to the Internet. This is especially true if an organization conducts business over the Internet. Any firewall should be "highly secure, [have] no noticeable network performance impact, [and have] maximum user transparency" (Connolly, 1996: 172).

Since intercepting messages through the Internet is the only method discussed that does not require someone to physically place a receiver near the computer or computer line, it has the least chance of being discovered. For this reason, it is the preferred method to access computerized information and requires the most attention for network security.

A system can be technically secure, and many papers have been written regarding this, such as "The Safety Catch" (Johnson and Tolly, 1995), "Network Security" (Snow and Chang, 1992), or "Operation Chain Link: The Deployment of a Firewall at Hanscom Air Force Base" (Conolly, 1996). An example of a network that needs to be secure is any network that carries classified information. Classified information is any information that has been deemed to be classified, based on the criteria in Executive Order 12958, 1995. Unclassified information is therefore any information that does not fall into one of the three above mentioned categories. However unclassified information may contain Essential Elements of Information (EEI), which is "information needed by an air commander to determine an offensive or defensive action" (Heflin, 1956: 191). While

classified systems are generally very secure, the same is not always true of unclassified systems. For financial reasons, unclassified systems tend to have less stringent security measures. Therefore the intelligence value of a system will be addressed next.

Intelligence Information

"The more dependent the adversary is on information systems for decision making, the more vulnerable he is to hostile manipulation of those systems" (Szafarsnski, 1995: 61). Any information can be attacked using one of four methods. These four methods, according to Howard, are:

1. Information Interception
2. Information Interruption
3. Information Modification
4. Information Fabrication

(Howard, 1997: 60-61)

The following sections explore each of these four methods of attack and their value, both positive to the attacker and negative to the Air Force system being attacked.

Information Interception. Information Interception is when "an unauthorized party gains access to an asset" (Howard, 1997: 60). An example of Information Interception is an adversary reading all of the messages passing into or out of a LAN or Intranet. According to Dr. David Probst, one of the primary advantage of Information Interception to an adversary is total situational awareness which leads to integrated battlespace management (Thrasher, 1996: 583-584). However, since there is no classified information on the system, all of the information on the system may be obtained through the Freedom of Information Act, except Privacy Act information. Information Interception will only allow for a faster assimilation of Essential Elements of Information (EEIs) and the gathering of information by an adversary will be unknown to the system administrator. While information can be encrypted to prevent Information

Interception, the information will still have to be handed over when requested through the Freedom of Information Act. The advantage of encryption is slowing down the assimilation of EEIs by an individual and that the system administrator, and the commander, will know what information has been disseminated.

Information Interruption. Information Interruption is when "an asset of the system is destroyed or becomes unavailable or unusable" (Howard, 1997: 60). An example of Information Interruption is an adversary preventing any messages from passing between a LAN or Intranet and the Internet. The main advantage to an intruder of Information Interruption is slowing down or preventing an Air Force organization from accessing their own information (Schwarteau, 1996: 535) (Thrasher, 1996: 581). Therefore, the information must be transferred to the organization needing it using a secondary system, if available. This will slow down the Observation-Orientation-Decision-Action (OODA) Loop or reduce the situational awareness of the Air Force commander. In addition, the secondary system may be more vulnerable to Interception, Modification, Fabrication, or further Interruption.

Information Modification. Information Modification is when "an unauthorized party not only gains access to, but tampers with an asset" (Howard, 1997: 60). An example of Information Modification is an adversary who changes some messages as the messages they pass from the Internet to a LAN or Internet, such as an order telling a commander to move three aircraft is changed to 30 aircraft. Information Modification can confuse the commander by denying correct information and replacing it with false information. In this event all of the information received from this information system is suspect and for all practical purposes Information Interruption has occurred. The most serious damage is if Information Modification has occurred and this has not been detected (Thrasher, 1996: 580-581). This vulnerability can be partially overcome by encrypting

information. Assuming that the passwords are secured, this will insure that information has not been modified from the source to the receiver (Schwarteau, 1996: 534).

<u>Information Fabrication</u>. Information Fabrication is when "an unauthorized party inserts counterfeit objects into the system" (Howard, 1997: 60). An example of Information Fabrication is an adversary who creates messages and inputs them into a LAN or Intranet from the Internet so that the fabricated message appears to come from a legitimate user, such as the unit's headquarters. Information Fabrication is similar to Information Modification except that the correct information has not be eliminated. Information Fabrication can still confuse the commander providing false information. In this event all of the information received from this information system is suspect and for all practical purposes Information Interruption has again occurred. As in Information Modification, the serious damage is when Information Fabrication has occurred and this has not been detected (Thrasher, 1996: 580-581). This vulnerability can also be partially overcome by encrypting information. Assuming that the passwords are secured, this will insure that information is from the source that it claims to be from (Schwarteau, 1996: 534).

Legal Information

This section will address two areas. The first area covers what a system administrator is allowed to monitor. The second area covers the areas that will be required before the U.S. Attorney can prosecute an individual who has broken into an Air Force system. According to (Soma and others, [1994]: 3-7) there are laws and regulations governing Air Force Computer Security stemming from:

1. International Treaty
2. Federal Law
3. Presidential Directive
4. DoD Policy

5. Air Force Policy

6. Local Policy

These rules are products of a series of treaties, laws, directives, and policies. While these rules do affect a computer system, an individual attempting to break in to a system is not likely to care. For example, an individual attempting to break in to a system will not care what the local policy of the Major Command (MAJCOM) is, however those in that command must follow MAJCOM policies and procedures. Also, when those in a MAJCOM violate their policies and procedures, they can be held responsible. On the other hand there is no MAJCOM punishment for the individual attempting to break into a system violating only the MAJCOM policies. As a result, a system administrator must know what it is legal to monitor, and what information is required to prosecute someone who gains unauthorized accesses to an Air Force system.

The Legal Guide to Computer Crime: A Primer for Investigators and Judge Advocates by Lt Col Soma and others, is a reference guide created by the Air Force Office of Special Investigations, Office of the Staff Judge Advocate to "provide a framework for Agents and lawyers to use in the investigation and prosecution of computer crime cases" (Soma and others, [1994]: i). Since this publication also incorporates a large amount of case law, and due to a lack of any other consistent publications, this publication has been chosen as a sole source. Information in this section was reviewed by the Wright-Patterson Air Force Base Legal Office for accuracy and currency.

Monitoring. "It is permissible for the system operator to create an audit trail of systems the subject has entered or attempted to enter. This use is specifically permitted... if no content is ascertained" (Soma and others, [1994]: 16). This gives a system administrator or manager permission to log everywhere an individual has visited but not what that person has done there. One exception is made for "the system operator to the

extent necessary to manage the system used to end electronic communication (e-mail)" (Soma and others, [1994]: 23). This gives a system administrator permission to monitor everything occurring on a system to insure that it is working properly. This is similar to the fact that the telephone company can listen to phone conversations to insure that their lines are working properly and logs the duration of all calls as well as the number called. The phone company may not listen in on an individual's conversation or log the communications that passes over these phone lines. Unlike the telephone company, any message obtained either inadvertently or through routine system monitoring that appears to pertain to a crime may be disclosed to law enforcement agencies and used without a warrant (Soma and others, [1994]: 23).

Prosecution. If someone breaks into an Air Force computer system, three items are desired in order to prosecute this individual. The first two desired items are Banners and Passwords, which will be explained in the following section. The third item, which is required, is an Audit Trail. While an Audit Trail can be obtained independent of the Banners and Passwords, it may be legally useless without both of them (Muldoon, 1997). Therefore the Audit Trail is placed within the Banners and Passwords in this section.

Banners. A Banner is a piece of information, normally text, that is displayed upon accessing a system that informs a user that only authorized personnel may use the system and with no expectation of privacy on the system. A Banner "should be included on all Air Force systems" (Soma and others, [1994]: 18). Without a banner, an individual has an expectation of privacy, and the monitoring of a system without a warrant is not allowed (Soma and others, [1994]: 18). How much of an individual's information stored on a computer is private must be determined on a case by case basis. It is clear that a file posted on a common network drive contains no expectation of privacy (Soma and others, [1994]: 18-19). A banner that is commonly used in the Air Force to reduce the expectation of privacy is:

This is a Department of Defense (DoD) computer system. DoD computer systems are provided for the processing of Official U.S. Government information only. All data contained on DoD computer systems is owned by the Department of Defense, *and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner*, by authorized personnel. **THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM.** System personnel may give to law enforcement officials any potential evidence of crime found on DoD computer systems. ***USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, or CAPTURING and DISCLOSURE.***

IF YOU DO NOT CONSENT, LOG OFF NOW.

Another banner that is commonly used in the Air Force to reduce the expectation of privacy and to display who has the authority to operate an Air Force system is:

****WARNING****

DOD COMPUTER SYSTEMS ARE PROVIDED FOR THE PROCESSING OF OFFICIAL U.S. GOVERNMENT INFORMATION ONLY. USE OF THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS. SYSTEM WILL BE MONITORED TO ENSURE INFORMATION SECURITY, SYSTEM INTEGRITY, AND THE LIMITATION OF USE TO OFFICIAL PURPOSES. THE USE OF DOD COMPUTER SYSTEMS CONSTITUTES CONSENT TO MONITORING AS AN INTEGRAL PART OF SYSTEM MANAGEMENT. INFORMATION DERIVED FROM SYSTEM MONITORING MAY BE USED AS A BASIS FOR ADMINISTRATIVE, DISCIPLINARY, OR CRIMINAL PROCEEDINGS. IF YOU DO NOT CONSENT TO CONTINUED MONITORING OR ARE NOT AN AUTHORIZED USER OF THIS SYSTEM, EXIT THIS SYSTEM NOW.

****YOUR USE OF THIS SYSTEM IS BEING MONITORED****

(Soma and others, [1994]: Atch. 2)

Passwords. A password is information required upon logging into a system to verify the user's authorization to use a system. Passwords, although a barrier to entry on one hand, are also very important to prosecute someone who is illegally

accessing an Air Force computer system. Since the individuals "gain access to a program by falsely representing themselves as an officer or employee of the United States," (Soma and others, [1994]: 5) they may be prosecuted. There is no requirement that this individual steal anything of value, simply that the "statement [falsely representing themselves] was 'knowingly' and 'willfully' made" (Soma and others, [1994]: 5). Without a password securing the system, it must be proven that something of value was stolen (Soma and others, [1994]: 4). This process can be a complex, and will be covered in more detail later in this chapter.

Audit Trail. An Audit Trail is a trace of what information a user has accessed on a system. While an Audit Trail can be used for legal purposes, it is also very useful in attempting to trace hardware or software difficulties. As was mentioned at the beginning of this section, "It is permissible for the system operator to create an audit trail of systems the subject has entered or attempted to enter. This use is specifically permitted ... if no content is ascertained" (Soma and others, [1994]: 16). Therefore, an Audit Trail can be very useful to law enforcement to investigate a crime that has already occurred. Depending on the locations that an intruder accesses and his access times, it is possible for a U.S. Attorney to prove that an intruder knew that he was not allowed access to a system and entered, regardless of the presence of a Banner or Password. The presence of a Banner and Password make the U.S. Attorney's prosecution less difficult and more persuasive, however the Audit Trail is all that is required (Muldoon, 1997). Since an Audit Trail contains only context, locations and times without content, it falls under the same authority as a similar device most people are familiar with, caller ID (Soma and others, [1994]: 15). An Audit Trail can be very useful because "if caller ID [Audit Trail] is already installed and the phone call recipient [system administrator] consents to reading of the device, no warrant or search authority is necessary. On the other hand, if the caller ID [Audit Trail] is installed during the course of an investigation,

the safer approach is to obtain proper search authority or a warrant" (Soma and others, [1994]: 15).

Costs of Secure and Insecure Systems

A limiting factor for any commander when considering the security of a computer system is the cost to improve the system's security. This must be weighed against the cost to maintain a system with a small amount of security, or no security in a cost/benefit analysis. Therefore, this section will break down the cost into the of an unsecured system

Cost of Insecure System	Insecure System	Secure System
Maintenance	Generally lower, unless damaged by an intruder	Higher due to system complexity
Accessibility	Open to all	Restricted
Intelligence	Value of information stolen, may compromise national security (high cost)	Prevention of compromise of national security information
Speed	Generally Faster, unless damaged by an intruder	Slower

Figure 4. Costs of Secure and Insecure Systems

versus the cost to secure a system. This may be seen in Figure 4.

The cost of an insecure system can be broken into two areas. The first area is the cost to repair a system after it has been attacked. Added to this is the cost in time of a system not operating at its optimal performance. The final cost is the value of the information that has been intercepted.

Maintenance and Speed. The repair costs for a system after an attack is currently the most common method of determining a piece of information's value. This is the cost, in either man hours or dollars, for the system administrator to un-corrupt any

corrupted files after an information attack. It also includes the cost required for the system administrator to patch the hole that an attack occurred through, to insure that another identical attack is not possible (Thatcher, 1997).

The loss of an information system or the degrading of its performance can be a serious cost. As the Air Force Chief of Staff said, "If you can analyze, act, and assess faster than your opponent, you will win" (Fogleman, 1995: 31). This refers to the OODA loop, in which the efficient flow of information is vital. The first "O" refers to observing. Information allows a commander to "see" what is happening, and information systems allow the fast and efficient passing of this information. The second "O" is orienting. Information systems improve the sorting of the information that is being observed to aid a commander. Again, the fast, efficient, and effective operation is critical. The "D" is the decision that a commander makes. The "A" stands for acting. Just as information systems passed observations to the commander. These systems must also pass the decision to subordinate units in a fast and efficient manner so that they may carry out the action (Minihan, 1994: 17). If any of the four portions of the OODA loop are broken, a commanders actions will be impaired. In some cases this will simply be an inconvenience, and in some cases this will be a loss of resources, resources which may prove vital to an Air Force organization.

Intelligence Value. The value of the information stolen is often very difficult to determine. It could be determined by the cost to initially collect the information. This would seem to make sense for technical material, but not if the information is travel schedules which are used to conduct a terrorist act. Therefore, the specifics of this section are still up for discussion. The only guidance in determining the value of information is that "classified information [must] have controls that prevent access by unauthorized persons, and ensure the integrity of the information" (Executive Order 12958, 1995: 17).

Cost of Secure System. The cost of a secure system can be broken into two areas. The first area is the monetary cost to improve the security of a system. The second, which is equally important, is the cost in time of a system not being operating at its optimal (insecure) performance.

Maintenance. The monetary cost to secure and maintain a system consists of the cost of installing a firewall, or possibly the cost of changing the network architecture to incorporate a more secure topology. While some of these measures might be quite expensive, that must be weighed against the costs of an insecure system. It is estimated that "protection [constitutes] only about 7 percent of information systems costs and only about 0.2 percent of the cost of forces. Such and investment, in effect, protects the outlay for all forces" (Busey, 1994: 15).

System Speed and Accessibility. The time cost to secure a system can be broken into three main areas. The first area is the time cost for the system administrator to install a secure architecture. This area also includes initial training of all individuals operating on a new system. The second time cost is in maintaining a secure system and instructing new employees how to operate the system. The final time cost is the most difficult to quantify. This is the time cost of operating a secure system. The best example is logging on to a system. It takes additional time to type in your password, but this additional time greatly increases the system's security. The determination of the point when the increase in time is not worth the security is a management decision, and this determination leads to an important constraining factor in the management decision (Minihan, 1994: 15).

Interested Organizations

In 1988 it was realized, due to an attack, that the Internet was vulnerable to a coordinated security attack. In response to this attack, known as the Internet Worm,

ARPA established the Computer Emergency Response Team (CERT) (Harvey, 1991: 167) (Fithen and Fraser, 1994: 108).

Computer Emergency Response Team (CERT). The CERT, located at Carnegie Mellon University's Software Engineering Institute, has become the focal point for Internet security. They are "concerned with computer security, by which is to be understood the integrity of information, the functionality of the network, the confidentiality of information, and the correct use of resources" (Harvey, 1991: 167). As the Internet has continued to grow, many organizations have established their own internal CERT, such as AFCERT by the Air Force.

Forum of Incident Response and Security Teams (FIRST). In response to many organizations forming their own CERTs, it quickly became apparent that these CERTs would need to coordinate their operations. To meet this need, the Forum of Incident Response and Security Teams (FIRST) was established. FIRST currently consists of 61 CERTs and other interested parties, such as Apple Computer, from 13 countries (FIRST team-info, 1997: 1-10) (FIRST about, 1997: 1).

Summary

This chapter discussed the three areas that a manager needs to consider when making a decision about network security. The first factor is the technical vulnerabilities of a computer network, based on the connectivity of the system. The second factor is the intelligence values of the computer system. The third factor is the legal information required to prosecute an individual gaining unauthorized access to the system. From these factors, the model in Figure 5 is proposed, and will be discussed in greater detail in Chapter Four.

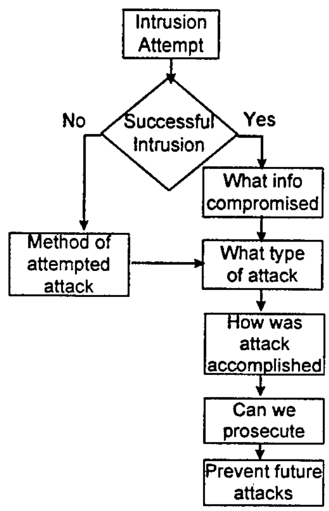

Figure 5. Initial Overview Model for Determining Information to be Captured Regarding Unauthorized Computer Entry

III. Methodology

Chapter Overview

This thesis develops a model for the information to be captured about an unauthorized intrusion into a computer network. It then tests this model through two iterations of a Delphi process. Changes to the model based on the Delphi process are incorporated and a final model is proposed.

Management Decision Model

The "Model for Determining Information to be Captured Regarding Unauthorized Computer Entry" is developed in Chapter Four from the literature review in Chapter Two. The model is then modified and validated in Chapter 4 by comments from experts in the field using the Delphi method.

Validation of the Management Decision Model

Description of Delphi. The Delphi technique originated in an Air Force-sponsored RAND Corporation study in the mid 1960's. The Delphi process is "a set of procedures for eliciting and refining the opinions of a group of people" (Dalkey, 1967: 1). Group members consist of experts in the field. The use of multiple experts is based on the age-old premise that "n heads are better than one" (Dalkey, 1969: 6). The procedures were designed to reduce the negative aspects of committees, through characteristics such as anonymity and controlled feedback (Dalkey, 1967: 3). A description of a typical use of Delphi is:

> A typical exercise is initiated by a questionnaire which requests estimates of a set of numerical quantities, e.g., dates at which technological possibilities will be realized, or probabilities of realization by given dates, levels of performance, and the like. The results of the first round will be summarized, e.g., as the median and inter-quartile range of the responses, and fed back with a request to revise the first estimates where appropriate. On succeeding rounds, those individuals whose answers deviate markedly from the median (e.g., outside the inter-quartile range) are requested to justify their estimates. These justifications are summarized, fed back, and

> counter-arguments are fed back and additional reappraisals collected. This basic pattern has, of course, many possible variants, only a few of which have been tried. (Dalkey, 1967: 4)

Reasons for using Delphi. The Delphi method has been chosen to validate the model to gather expert opinion and bring the expected diversity of opinions to a convergence. It was also chosen because it was designed to arrive at efficient operational model based on an initial model (Brown and Helmer, 1964: 1-2).

Choice of Experts. "We use experts because [the expert] has at his disposal a large store of background knowledge and a cultivated sensitivity to its relevance which permeates his intuitive insight" (Brown, 1968: 13). The experts chosen are the U.S. members of the Forum of Incident Response and Security Teams (FIRST). This group of organizations was chosen because they deal with computer security issues daily and represent "a variety of computer security incident response teams from government, commercial, and academic organizations" (FIRST about, 1997: 1). Only U.S. members of FIRST were chosen due to possible differences in importance of factors outside the U.S., since some of the countries with FIRST members do not contain a free market economy. A list of these U.S. organizations may be found in Appendix B.

Approach. This research will use a modified Delphi, in that the only question asked will be: Review the model and make comments on how the model may be improved. Therefore, there will be no statistical group response, simply an incorporation of improvements to the model and comments regarding reasons for the changes.

The model along with a paper explaining the purpose of the research, will be distributed using electronic mail (e-mail) to U.S. members of FIRST. Comments and improvements from responding organizations will be incorporated into the model. This improved model will then be returned in a second round of the Delphi technique to the same experts for additional comments and improvements. This process will be repeated

until a consensus or lack of significant change occurs. These changes will then be incorporated into the final model.

IV. Results

Chapter Overview

Chapter Four proposes an initial model of information to be gathered about unauthorized computer system entry based on information gathered during the literature review. Responses to the delphi process are then discussed and the model is modified based on this feedback.

Areas Considered by a Manager

There were five factors discussed in Chapter Two that a manager needs to consider when making a decision about network security. These five factors are technical vulnerabilities of a computer system, the intelligence value of the information in the system, the legal information required to prosecute an individual illegally accessing the system, the cost of a secure versus insecure system, and the legal requirements for an Air Force system. The first three factors are considered inputs to a manager's decision. These are considered inputs since the manager has control over these areas. The final two areas are controlling factors. Controlling factors are areas that a manager must abide by, and generally can not control. The cost of a secure versus insecure system is included here since a manager does not control the amount of the budget, but may control where to spend the money. This can be seen in Figure 6.

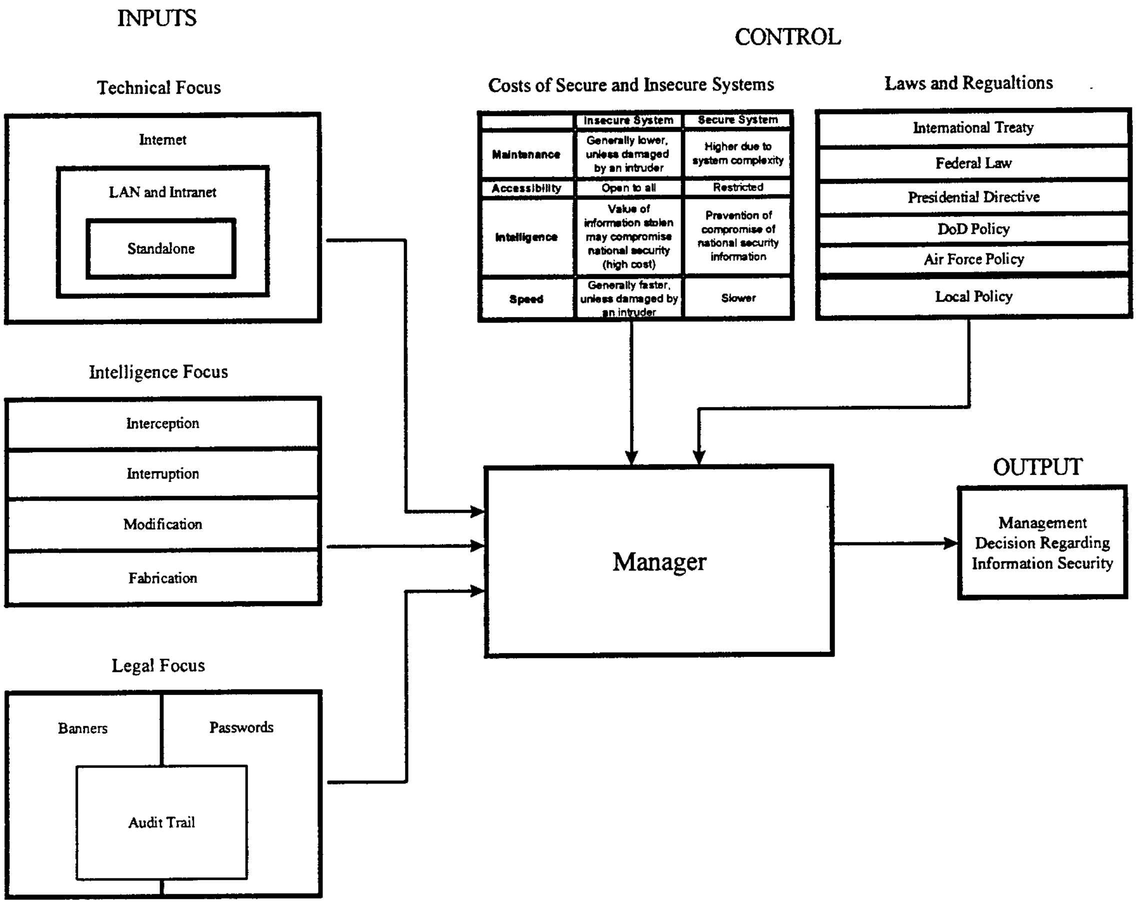

Figure 6. Areas Considered by a Manager to Make a Decision Regarding Information Security

Initial Model

In order for an Air Force manager to be able to make decisions as listed above, certain information must be captured. The areas in which a manager must have information are summarized in the model shown in Figure 7.

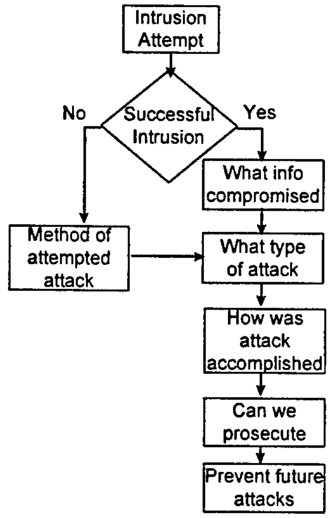

Figure 7. Initial Overview Model for Determining Information to be Captured Regarding Unauthorized Computer Entry

Intrusion Attempt. Once an intrusion has been attempted, it must be decided whether the intrusion was successful. If it was unsuccessful, noting the type of attack in a database may by useful for future analysis and comparison with other organizations. If the intrusion was successful, then information must be gathered in several additional areas. This would include the type of attack and what information was compromised, the method of the attack, whether the attackers can be prosecuted, and what may be done to prevent future attacks. With this information, a manager will be able to make an informed decision regarding the unauthorized computer entry. Each of these areas will now be examined in greater detail.

Successful Intrusion Determination. It must first be determined that there was an attack, and whether or not it was successful. If the attack was successful, then there is additional information to be gathered regarding the attack. If the attack was not successful, then learning about the type of attack may help evaluate future attacks. If it is unclear whether or not the attack was successful, it is better to follow the assumption that the attack was successful.

If the attack was successful, it is important to determine what has been compromised. This information will be used repeatedly in other areas, such as in the type of attack.

What Information was Compromised and What Type of Attack. It must be determined what type of attack has occurred. A manager should acquire information in the following areas:

1. If the attack involved the interception of information:
   a. What information has been intercepted?
   b. Who does this information affect?
   c. How important is it that this person obtained access to this information?
2. If the attack involved the interruption of information:
   a. What information has been interrupted?
   b. Who/what does this interruption affect?
   c. Can the information be replaced?
   d. How important is this loss of information?
3. If the attack involved the modification of information:
   a. What information has been modified?
   b. Can this information be repaired or replaced?
   c. How important is this modification of information?
4. If the attack involved the fabrication of information:
   a. What information has been fabricated?
   b. Who/what may have been affected by this fabricated information?
   c. How important is the existence of this fabricated information?

How the Attack was Attempted. A manager should analyze how the attack was accomplished. A manager should acquire information in the following areas:

1. For every attack on a stand-alone system:

a. The method of attack used.

b. If the attack used emissions:

(1) Shielding of the system.

c. If the attack used physical access:

(1) Organization's security practices.

2. For every attack on a Intranet/LAN:

a. The method of attack used.

b. If the attack used physical access:

(1) Organization's security practices.

c. If the attack used emissions:

(1) Shielding of nodes and links.

(2) Encryption of messages and type of encryption.

3. For every attack on a system connected to the Internet:

a. The method of attack used.

b. If a message was intercepted external to the organization:

(1) Encryption of messages and type of encryption.

c. If attack occurred through the firewall:

(1) Strengths and weaknesses of the your firewall.

Possibility of Prosecution. A manager should know information regarding possible prosecution of the attackers. A manager should acquire information in the following areas:

1. Is a banner shown at log-in:

a. Indicating entry is limited to authorized personnel, and that it is illegal for others to gain access to the system.

b. The users actions may be monitored.

2. Has the attacker represented himself as someone else, such as logging in using someone else's password.
3. Is there a log tracing the actions of the attacker.

Preventing Future Attacks. A manager should know information about how future attacks may be prevented. A manager should acquire information in the following areas:

1. Possible realignment of current assets used to secure the system.
2. Are additional assets required and available.

Conclusion. When all of this information has been captured, then a manager of an Air Force system will be able to make an informed decision regarding unauthorized computer entry.

Figure 8 embodies the entire process that a manager will follow to determine the information to be captured regarding unauthorized computer entry.

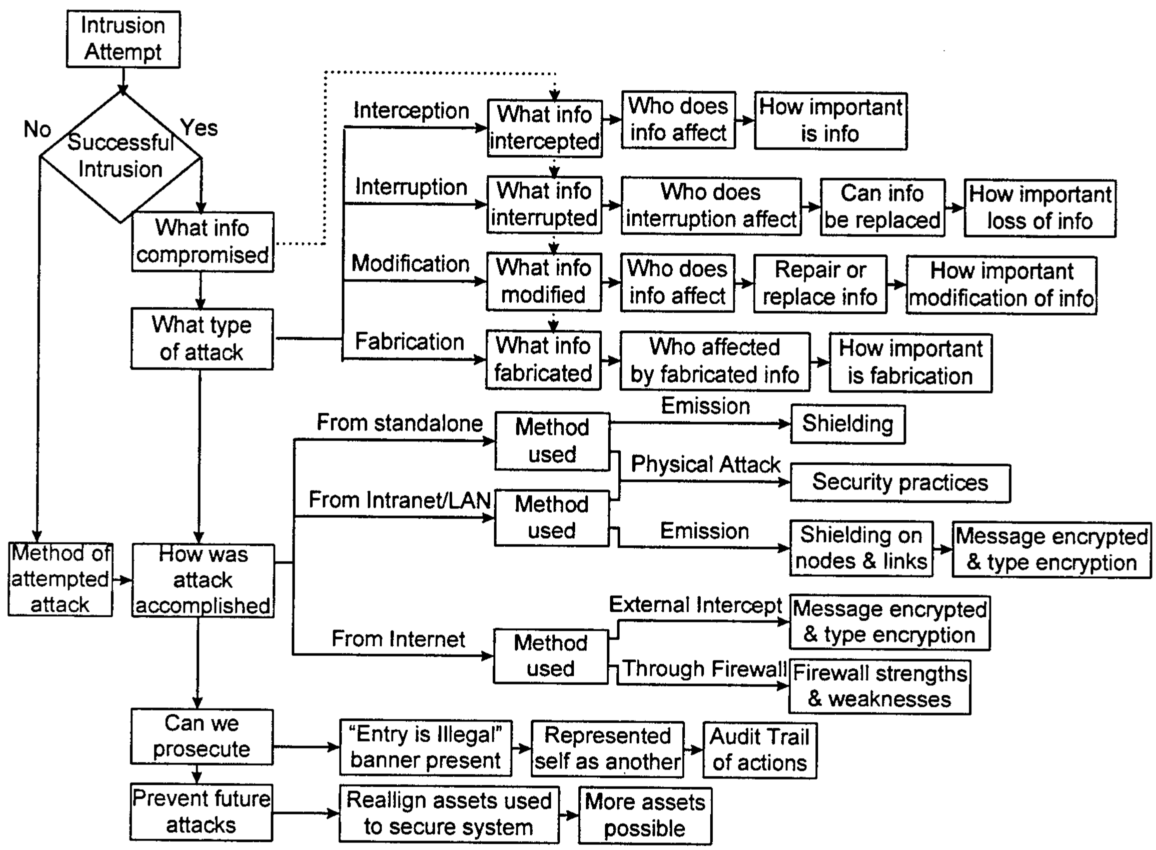

Figure 8. Initial Model for Determining Information to be Captured Regarding Unauthorized Computer Entry

Model After First Round of Delphi

Based upon inputs from the first round of delphi, several modifications were made to the model. The first change was replacing "attack" with "intrusion." This change was made since an intrusion is easier to define than an attack. An attack requires intent, which is not known by the system administrator Another change was defining an intrusion attempt and a successful intrusion. An intrusion attempt is defined as an act which is intentionally employed for the purpose of gaining unauthorized access to a

computer or computer system. A successful intrusion is defined as an act which is intentionally employed for the purpose of and is successful at gaining unauthorized access to a computer or computer system.

Under the "What Information was Compromised and What Type of Attack" section, another type of attack was added. This is a probe, where no information is interrupted, intercepted, modified, or fabricated.

In the section discussing "How the Attack was Accomplished," now "How the Intrusion was Accomplished," intrusions using emissions was expanded to include both intentional shielding of the system and unintentional shielding of the system due to its location. If the intrusion used physical access, then information regarding computer security policies was added to information about the organization's security practices. If the intrusion occurred from a system connected to the internet through the firewall, information about the use of guest login was added. Information regarding intrusion through a modem was added, requiring information regarding the organization's security practices, their policies regarding computer security, and their use of guest login.

The section "Is Prosecution Possible" was renamed to "Report to Law Enforcement," since it was thought that this was a more adequate description. Information was also added to this section whether the appropriate CERT had been notified of the intrusion attempt.

The final modification was the addition of information in the section "Preventing Future Attacks" about the installation of available security patches.

Finally, punctuation and section headings were added to improve the readability of the model.

All of these changes may be seen in the improved model in Appendix F. Second Model Sent to Delphi Participants on page 60. It is also summarized in Figure 9.

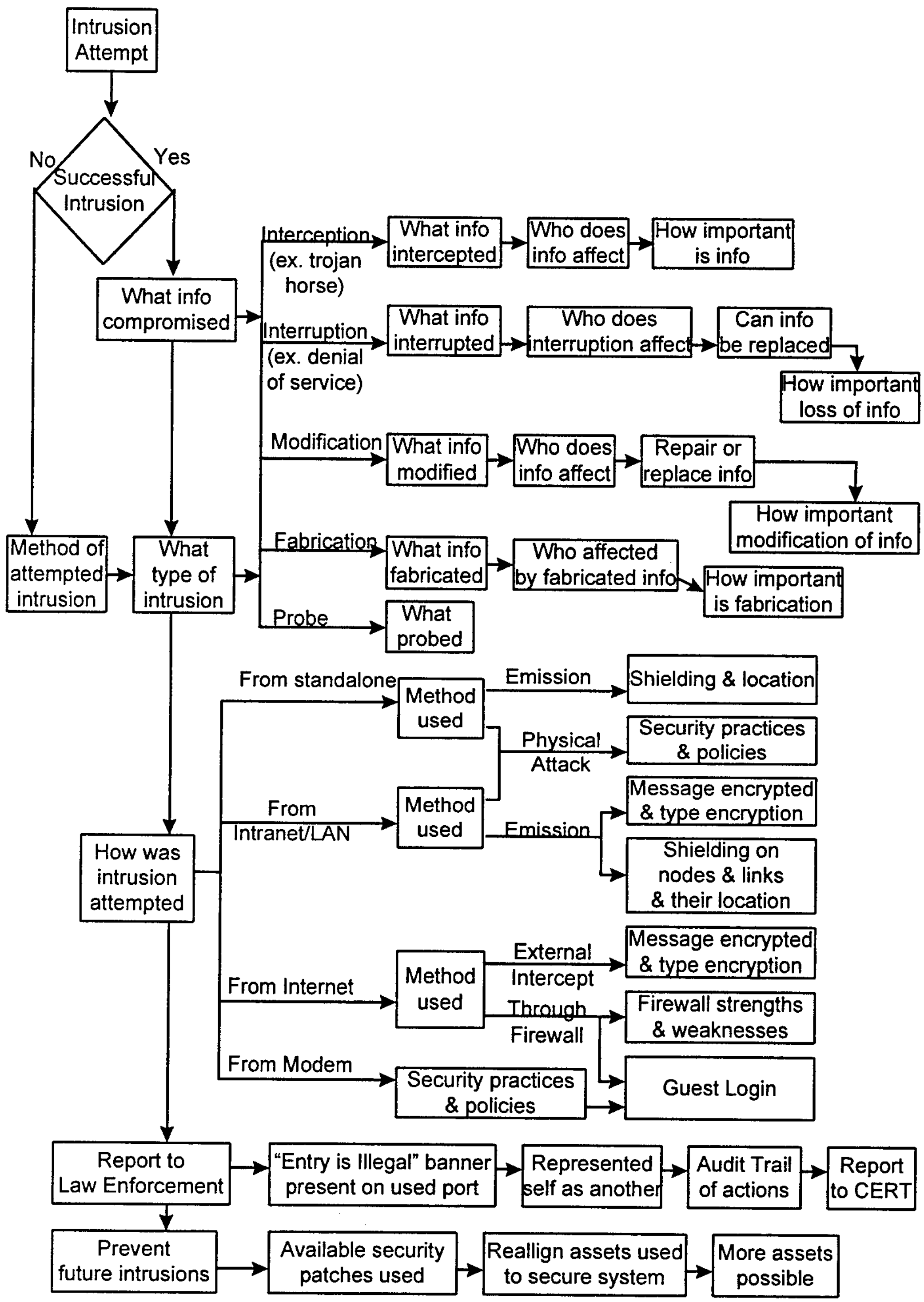

Figure 9. Model After First Round of Delphi for Determining Information to be Captured Regarding Unauthorized Computer Entry

Model After Second Round of Delphi

Based upon inputs from the second round of delphi, a few minor modifications were made to the model. The first change is pointing out that the order that the information should be gathered in will change based on the situation. For example, in some situations it is more important to prevent future intrusions, then determine what was compromised. There were also other comments on formatting and punctuation. Another comment is a limitation of the research, it was not designed to cover insider misuse. All of these changes may be seen in the improved model in Appendix G. Final Model on page 66.

Since there were no major modifications to the model based on inputs from the second round of delphi, no further rounds of delphi are required.

Summary

This chapter presented an initial model of information to be gathered about unauthorized computer system entry based on information gathered during the literature review. Responses to the delphi process were then discussed and the model was modified based on this feedback. The next chapter will present the conclusions and recommendations which have been drawn from this information.

V. Conclusion

Chapter Overview

Chapter Five discusses the results presented in Chapter IV. Results, including their significance for operational implementation and recommendations. It presents limitations of the study and recommendations for future work.

Discussion

As the model was reviewed by experts, there were several areas of the model that were modified based on their inputs.

Information on "Guest Login" was added to "How was intrusion attempted." Many computer systems have a guest login option. This is normally used by individuals visiting an organization so that they can have temporary access to the network without bothering the network administrator. For these accounts, the user-name and password are normally simple, such as "user" and "guest." Once someone has logged into the system, they are then free to operate as a normal user. Since these accounts normally have very few safeguards, they normally only have limited access. If an intrusion occurs from one of these accounts, the network administrator will want to know additional information about the access on that account.

Information about a Probe was added under "What type of intrusion." In the initial model, an attack was only considered successful if information was intercepted, interrupted, modified, or fabricated. Under this definition, someone who successfully gained unauthorized access and did not bother any information was not considered an attack.

Experts reviewing the model recommended that after an unsuccessful intrusion attempt, the "Method of attempted attack" should flow into "What type of intrusion" instead of "How was intrusion accomplished." This was recommended since there have

been instances where it was possible to ascertain what type of intrusion was being attempted, even though the intrusion was not successful.

The information originally gathered on shielding of computers, nodes, and links was expanded. It was pointed out that there are two different types of shielding. The first type of shielding is shielding that was intentionally placed around a computer, node, or link in order to reduce its emission. The second type of shielding is unintentional shielding. A computer operated in the basement will have more natural shielding than one operated on the top floor of a building. While the location may or may not be intentional, information on this shielding was determined to be important.

Information was gathered on "Security practices" was expanded to include "Security practices and policies." There was some concern by experts that this was too narrow. This is because "Security practices" describe what security measures are actually taken by individuals within the organization. Therefore, "Security practices" was expanded to "Security practices and policies." This includes not only the security measures that individuals take, but also what security measures the organization teaches.

Another area of concern is the issue of multiple methods of access. It was brought up by several of the experts in the field that one of their largest problems is unauthorized connections between their computer system and other computer systems. Very often, these connections are not only unauthorized, but also unknown to the system administrator until after an intrusion has occurred. An example provided by one expert was a modem linked to an individuals desktop computer, linked to the organization's network. That modem provided free access to the organization's network and access to the information on the network to anyone who new the correct phone number. It is stories of security violations such as this that strike fear in the heart of every network administrator. Only be educating users of the possible risks of their actions and by

establishing timely and (for the user) simple solutions to their problems can these security violations be avoided.

Information about "Available security patches used" was added to "Prevent future intrusions." It was originally felt that information about whether the system had all available security patches installed fell under "Realign assets used to secure system." However this was reported by experts as not being clear, therefore this information was broken out into a separate item.

The order for the collection of this information was determined to vary depending on the specific situation of the successful intrusion. The model was laid out so that the information required was in a logical progression for an attack. However, examples were provided by experts showing where the order of information gathering would change. In these situations, the speed that the information was gathered was important. The model was then changed so that, while all of the information was still required in order to make an informed decision, the order was no longer important and is allowed to vary depending on the situation.

It was pointed out by one expert that in some situations: "Good information today is better than perfect information tomorrow." It was also pointed out that there were often inaccuracies in the information about an intrusion that occurred between where the intrusion occurred and the CERT. This insight lead to the recommendations made in the section below.

It was recommended by one of the experts that this thesis be expanded to include insider misuse. This thesis covers only external facets of computer security. However, recognizing the value of exploring other level of risk leads to suggestions for further research.

Recommendations

In the rapidly changing world of computer security, two of the major themes that were recognized and addressed by the experts who commented on this model included timeliness and accuracy of information. In order to fully utilize the information that this model has established as important to the manager of a computer system, the following recommendations are made:

1. The information should be captured by the individual as close to the intrusion as possible. This is done to reduce the inaccuracy of the information.
2. The information should be passed in a timely and accurate manner to the organization's CERT.
3. The CERT should use the information to attempt to rectify the intrusion.
4. The CERT should conglomerate the information in an attempt to evaluate the possibility of an organized intrusion attempt.
5. The CERT should pass relevant information to other system administrators in an attempt to prevent future successful intrusion attempts.

Limitations

This thesis is focused on the military, and specifically on the Air Force. Comments on the model were received from all of the CERTs within the DoD. However, some insight might have been obtained from non-DoD CERTs. Of the forty-seven non-DoD experts chosen, only a little over twelve percent had the spare time to evaluate the model and provide feedback. This small response may be because all communication with the CERTs (except AFCERT) was done using only electronic mail. Since comments were received from all of the DoD CERTs, the small feedback from non-DoD CERTs is considered acceptable.

This thesis is focused on the management aspects of unauthorized computer entry. As a result, it did not deal with technical aspects of unauthorized computer entry or with

information security from authorized users. Exploring these other aspects of information security leads to suggestions for further research.

Recommendations for Future Research

This thesis developed a model for the information to be captured regarding unauthorized computer entry of an Air Force computer system. Future research in this field could be focused on how to capture the information that was determined to be important in the model. Also, future research could attempt to weight the information in the model, to determine which information is the most important and why it is the most important. Finally, another avenue for future research is considering insider misuse of a computer network instead of only external intrusions into the system.

Summary

This thesis presented a model for data for the Air Force to use to capture information about unauthorized attempts to access computer systems. This model took a management focus, and incorporated the technical focus, intelligence focus, and legal focus as inputs into the management focus. An exploratory, qualitative methodology was used consisting an extensive literature review and interviews with experts in the field. These efforts produced the proposed model, which was reviewed by experts in the field using a delphi technique.

Appendix A. Glossary of Acronyms

AFCERT—Air Force Computer Emergency Response Team

ARPA—Advanced Research Projects Agency

ARPANET—Advanced Research Projects Agency Network

ARPA/IPTO—Advanced Research Projects Agency's Information Processing Techniques Office

ASIM—Automated Security Incident Measurement

CERT—Computer Emergency Response Team

DISA—Defense Information Systems Agency

DoD—Department of Defense

EEI—Essential Elements of Information

e-mail—electronic mail

FIRST—Forum of Incident Response and Security Teams

LAN—Local Area Network

MAJCOM—Major Command (Normally between HQ AF and Numbered Air Forces)

OODA—Observation-Orientation-Decision-Action

TCP/IP—Transmission Control Protocol and Internet Protocol

U.S.—United States

Appendix B. U.S. members of the FIRST

1. AFCERT (US. Air Force CERT)
   Constituency: Air Force Users
   Email: afcert@afcert.csap.af.mil
   Telephone: 1 210-977-3157
   Pager: 1 800-854-0187
   Fax: 1 210-977-3632
   Membership Type: Full member

2. ANS CO+RE Systems, Inc. (ANS)
   Constituency: ANS Customers
   Email: anscert@ans.net
   Telephone: 1 313-677-7350
   Telephone: 1 313-677-7333 (emerg.)
   Fax: 1 313-677-7310
   Membership Type: Full member

3. Apple Computer
   Constituency: Apple Computer (worldwide)
   Email: first-team@apple.com
   Telephone: 1 408-974-6985
   Fax: 1 408-974-1560
   Membership Type: Liaison member

4. ASSIST US. Department of Defense Automated Systems Security Incident Support Team
   Constituency: DOD - Interest systems
   Email: assist@assist.mil
   Telephone: 1 800-357-4231
   Fax: 1 703-607-4735
   Membership Type: Full member

5. Bellcore
   Constituency: Bellcore
   Email: skoudis@cc.bellcore.com
   Telephone: 1 908-758-5676
   Fax: 1 908-758-4504
   Membership Type: Full member

6. Boeing CERT (BCERT)
   Constituency: Boeing
   Email: compsec@pss.boeing.com
   Telephone: 1 206-657-9353; 206 657-9377

Telephone: 1 206-655-2222 (emerg.)
Fax: 1 206-657-9477
Membership Type: Full member

7. CERT® Coordination Center (CERT/CC)
   Constituency: The Internet
   Email: cert@cert.org
   Telephone: 1 412-268-7090
   Fax: 1 412-268-6989
   Membership Type: Full member

8. CIAC US. Department of Energy's Computer Incident Advisory Capability
   Constituency: U.S. Department of Energy (DOE) and DOE Contractor sites, plus the Energy Science Network (ESnet). Also, National Institutes of Health (backup only)
   Email: ciac@llnl.gov
   Telephone: 1 510-422-8193, 24/7
   Fax: 1 510-423-8002
   Membership Type: Full member

9. Cisco Systems
   Constituency: Cisco Systems (employees/contractors)
   Email: first-team@cisco.com
   Telephone: 1 408 526-5638 or 1 408-527-3842
   Fax: 1 408 526-5420
   Membership Type: Full member

10. Digital Equipment Corporation Software Security Response Team - SSRT
    Constituency: Digital Equipment Corporation Customers and Digital Equipment Corporation Internal
    Email: rich.boren@cxo.mts.dec.com
    Telephone: 1 800-354-9000
    Telephone: 1 800-208-7940 (emerg.)
    Fax: 1 901-761-6792, 1 719-592-4121
    Membership Type: Full member

11. EDS
    Constituency: EDS and EDS Customers
    Email: jim.cutler@iscg.eds.com
    Telephone: 1 810-265-7514
    Fax: 1 810-265-3432
    Membership Type: Liaison member

12. General Electric Company
    Constituency: Thirteen GE businesses
    Email: Sandstrom@geis.geis.com
    Telephone: 1 301-340-4848
    Fax: 1 301-340-4639
    Membership Type: Full member

13. Goldman, Sachs and Company
    Constituency: Goldman, Sachs offices worldwide
    Email: shabbir.safdar@gs.com
    Telephone: 1 212-357-1880
    Pager: 1 917-978-8430
    Membership Type: Liaison member

14. Hewlett-Packard Company
    Constituency: All HP-UX and MPE Customers
    Email: security-alert@hp.com
    Membership Type: Full member

15. IBM-ERS IBM Emergency Response Service
    Constituency: IBM internal and external customers
    Email: ers@vnet.ibm.com
    Telephone: 1 914 759-4452 (8am - 5pm, EST/EDT (GMT-5/GMT-4))
    Telephone: 1 914 343-7705 (after hours)
    Fax: 1 914-759-4326
    Pager: 1 800-759-8352, PIN 1081136 (alphanumeric, two-way)
    Pager: 1081136@skytel.com
    Membership Type: Full member

16. MCI
    Constituency: MCI Employess, Contractors and Alliance Partners
    Email: 3557428@mcimail.com
    Telephone: 1 703-506-6294
    Pager: 1 800-SKY-8888 pin 216-2056
    Fax: 1 703-506-6281
    Membership Type: Full member

17. Motorola Comp. Emergency Resp. Team
    Constituency: Motorola
    Email: mcert@mot.com
    Telephone: 1 847-576-0669 (emerg.)
    Telephone: 1 847-576-1616
    Fax: 1 847-538-2153
    Membership Type: Full member

18. NASA Ames Research Center (Principle Center for Information Technology Security)
    Constituency: National Aeronautics and Space Administration
    Email: ais@ames.arc.nasa.gov
    Telephone: 1 415-604-6148
    Telephone: 1 415-604-1167
    Telephone: 1 415-604-6626 (emerg.)
    Pager: 1 415-428-9370
    Membership Type: Full member

19. NASIRC NASA Automated Systems Incident Response Capability
    Constituency: NASA and the International Aerospace Community
    Email: Nasirc@nasirc.nasa.gov
    Telephone: 1 800-762-7472 (U.S.)
    Telephone: 1 301-918-1970 (International) 7:00 am to 7:00 pm EST
    Pager: 1 800-SKY-PAGE Pin 2023056
    Fax: 1 301-918-8154
    Membership Type: Full member

20. NAVCIRT (Naval Computer Incident Response Team)
    Constituency: U. S. Department of Navy
    Email: navcirt@fiwc.navy.mil
    Telephone: 1 757-464-8832
    Telephone: 1 800-628-8893
    Telephone: 1 888-NAVCIRT (628-2478)
    Membership Type: Full member

21. NCSA-IRST (National Center for Supercomputing Applications IRST)
    Constituency: National Supercomputing Community, in particular our Industrial Partners, Collaborators, the State of Illinois, and K-12 Illinois Learning Mosaic community. Direct response for all systems in .ncsa.uiuc.edu and .ncsa.edu domains, and coordinate NCSA Mosaic or NCSA HTTPd security issues.
    Email: irst@ncsa.uiuc.edu
    Telephone: 1 217-244-0710 (24hr/7day)
    Fax: 1 217-244-7396
    Membership Type: Full member

22. NIH CERT US. National Institutes of Health
    Constituency: Employees of the U.S. National Institutes of Health
    Email: Kevin_Haney@nih.gov
    Telephone: 1 301 402-1812
    Telephone: 1 301 594-3278 (emerg.)

Fax: 1 301 402-1620
Membership Type: Full member

23. NIST/CSRC
    Constituency: NIST and civilian U.S. agencies (guidance only)
    Email: first-team@csmes.ncsl.nist.gov
    Telephone: 1 301-975-3359
    Fax: 1 301-948-0279
    Membership Type: Full member

24. NU-CERT Northwestern University
    Constituency: Northwestern University Faculty/Staff/Students
    Email: nu-cert@nwu.edu
    Telephone: 1 847-491-4058
    Fax: 1 847-467-5690
    Membership Type: Full member

25. OSU-IRT - The Ohio State University Incident Response Team
    Constituency: The Ohio State University
    Email: security@net.ohio-state.edu
    Telephone: 1 614-688-3412
    Pager: 1 614-292-1460 or email security@page.net.ohio-state.edu, first 2 lines of message will appear on pager.
    Fax: 1 614-292-7081
    Membership Type: Full member

26. PCERT Purdue Computer Emergency Resp. Team
    Constituency: Purdue University
    Email: pcert@cs.purdue.edu
    Telephone: 1 765-494-7844
    Fax: 1 765-494-0739
    Membership Type: Full member

27. Pennsylvania State University
    Constituency: Pennsylvania State University
    Email: krk5@psu.edu
    Telephone: 1 814-863-9533
    Fax: 1 814-865-3082
    Telephone: 1 814-863-4357 (emerg.)
    Membership Type: Full member

28. REACT - SAIC Rapid Emergency Action Crisis Team (REACT)
    Constituency: Commercial and government customers
    Email: react@cip.saic.com

Telephone: 1 888-REACT-1-2
Fax: 1 703-734-2234
Membership Type: Full·member

29. SBACERT - Small Business Administration
    Constituency: Small Business Administration offices and elements nationwide (U.S.A)
    Email: hfbolden@sba.gov
    Telephone: 1 202-205-6708
    Fax: 1 202-205-7064
    Membership Type: Full member

30. SGI Silicon Graphics Inc.
    Constituency: Silicon Graphics' User Community
    Email: security-alert@sgi.com
    Telephone: 1 415-933-4997
    Fax: 1 415-961-6502
    Membership Type: Full member

31. Sprint
    Constituency: Sprint Net (X.25) and Sprint Link (TCP/IP)
    Email: mike@sprint.net
    Telephone: 1 703-904-2430
    Fax: 1 703-904-2708
    Membership Type: Full member

32. SSACERT - U.S. Social Security Administration
    Constituency: U.S. Social Security Administration
    Email: ssacert@ssa.gov
    Telephone: 1 410 966-9075 or 1 410 965-6950
    Fax: 1 410 966-6230
    Membership Type: Full member

33. SUN Microsystems, Inc.
    Constituency: Customers of Sun Microsystems
    Email: chok@barrios.eng.sun.com
    Telephone: 1 415-786-4420
    Fax: 1 415-786-7994
    Membership Type: Full member

34. SUNSeT Stanford University Network Security Team
    Constituency: Stanford University Networks and Systems
    Email: security@stanford.edu
    Telephone: 1 415-723-2911

Fax: 1 415-725-1548
Membership Type: Full member

35. TRW Inc.
    Constituency: TRW Network and System Administrators
    Email: zorn@gumby.sp.trw.com
    Telephone: 1 310-812-1839
    Fax: 1 310-813-4621
    Membership Type: Full member

36. UCERT - UNISYS Computer Emergency Response Team (UCERT)
    Constituency: Unisys Internal/External Users
    Email: garygarb@unn.unisys.com
    Telephone: 1 215-986-4038
    Pager: 1 215-330-2316
    Membership Type: Full member

37. USHCERT - US. House of Representatives Computer Emergency Response Team
    Constituency: House Members, Officers, Employees, and Contractors
    Email: security@mail.house.gov
    Telephone: 1 202-226-6404
    Pager: 1 800-SKY-8888 pin 4719543
    Fax: 1 202-225-0368
    Membership Type: Full member

38. US. Veteran's Health Administration
    Constituency: Vet. Health Admin. Forum of Incid. Resp. Sec. Team
    Email: frank.marino@forum.va.gov
    Telephone: 1 304-263-0811, ext. 4062
    Telephone: 1 304-263-4748 (emerg.)
    Membership Type: Full member

39. Westinghouse Electric Corporation
    Constituency: Entire Corporation
    Email: smithce@westinghouse.com
    Telephone: 1 412-642-3040
    Emergency Telephone: 1 412-642-3444
    Fax: 1 412-642-3957
    Membership Type: Liaison member

Last modified 4 April 1997

(FIRST team-info, 1997: 1-10)

Appendix C. Initial Electronic Mail Message to Delphi Participants

Subject: Thesis Research

To: "AFCERT" <afcert@afcert.csap.af.mil>,
"ANS" <anscert@ans.net>,
"Apple Computer" <first-team@apple.com>,
"ASSIST" <assist@assist.mil>,
"Bellcore" <skoudis@cc.bellcore.com>,
"Boeing CERT (BCERT)" <compsec@pss.boeing.com>,
"CERT" <cert@cert.org>,
"CIAC" <ciac@llnl.gov>,
"Cisco Systems" <first-team@cisco.com>,
"Digital Equipment Corporation SSRT"
<rich.boren@cxo.mts.dec.com>,
"EDS" <jim.cutler@iscg.eds.com>,
"General Electric Company" <Sandstrom@geis.geis.com>,
"Goldman, Sachs and Company" <shabbir.safdar@gs.com>,
"Hewlett-Packard Company" <security-alert@hp.com>,
"IBM-ERS" <ers@vnet.ibm.com>,
"MCI" <3557428@mcimail.com>,
"Motorola Comp. Emergency Resp. Team" <mcert@mot.com>,
"NASA Ames Research Center (Principle Center for Information
Technology Security)" <ais@ames.arc.nasa.gov>,
"NASIRC" <Nasirc@nasirc.nasa.gov>,
"NAVCIRT" <navcirt@fiwc.navy.mil>,
"NCSA-IRST" <irst@ncsa.uiuc.edu>,
"NIH CERT" <Kevin_Haney@nih.gov>,
"NIST/CSRC" <first-team@csmes.ncsl.nist.gov>,
"NU-CERT" <nu-cert@nwu.edu>,
"OSU-IRT" <security@net.ohio-state.edu>,
"PCERT" <pcert@cs.purdue.edu>,
"Pennsylvania State University" <krk5@psu.edu>,
"REACT-SAIC" <react@cip.saic.com>,
"SBACERT" <hfbolden@sba.gov>,
"SGI" <security-alert@sgi.com>,
"Sprint" <mike@sprint.net>,
"SSACERT" <ssacert@ssa.gov>,
"SUN Microsystems" <chok@barrios.eng.sun.com>,
"SUNSeT" <security@stanford.edu>,
"TRW Inc" <zorn@gumby.sp.trw.com>,
"UCERT" <garygarb@unn.unisys.com>,
"USHCERT" <security@mail.house.gov>,
"US Veterans Health Administration"
<frank.marino@forum.va.gov>,
"Westinghouse Electric Corporation"
<smithce@westinghouse.com>

cc: "Dr. Heminger" <aheminge@afit.af.mil>,
"Maj. Vickery" <cvickery@afit.af.mil>

Dear Sir or Ma'am,

I am 1Lt Les Himebrook, a Graduate Student at the Air Force Institute of Technology, located at Wright-Patterson Air Force Base in Dayton, Ohio. I may be reached at 937-255-7777x2131, (DSN prefix 785 for military units), or <lhimebro@afit.af.mil>. My thesis advisor and program manager for Information Resource Management is Dr. Alan Heminger, who may be reached at 937-255-7777x3353, or <aheminge@afit.af.mil>.

My thesis topic is "Determining Information to be Captured Regarding Illegal Computer Entry." I have designed a model to accomplish this (attached as model.doc in Microsoft Word 7.0 or as model.txt in ASCII Text, without the two figures)

I would be very appreciative if you, as someone who works in the field of Information Security, would review my model and make comments on how the model may be improved. If possible, please return your comments by Thursday, September 25. I will then consolidate the comments and create an improved model. I will then send this improved model out for your assessment. In the improved model and my final thesis, no comments about the model will be attributed to particular individuals or organizations.

If you desire, a completed copy of my thesis can be sent to you, either by electronic mail (in Microsoft Word 7.0)or a paper copy. If you desire a copy, please let me know when you return your comments regarding my model

Thank you very much for your assistance.

LESLIE F. HIMEBROOK, 1Lt, USAF
Graduate Student, Air Force Institute of Technology

The model that was attached to this electronic mail message is located in Appendix D. Initial Model Sent to Delphi Participants on page 53.

Appendix D. Initial Model Sent to Delphi Participants

In order for an Air Force manager to be able to make decisions regarding unauthorized computer entry, certain information must be captured. The areas in which a manager must have information is summarized in the model shown in Figure 10.

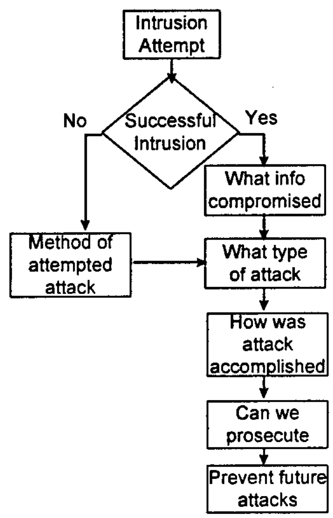

Figure 10. Initial Overview Model for Determining Information to be Captured Regarding Unauthorized Computer Entry

A manager begins this collection information process knowing certain information about his system even before there is an intrusion attempt. Once an intrusion has been attempted, it must be decided whether the intrusion was successful. If it was unsuccessful, noting the type of attack in a database may by useful for future analysis and comparison with other organizations. If the intrusion was successful, then information must be gathered in several areas. Information must be gathered about the type of attack and what information was compromised, the method of the attack, whether the attackers can be prosecuted, and what may be done to prevent future attacks. Once all of this information is captured, then a manager will have sufficient information to make an

informed decision regarding unauthorized computer entry. Each of these areas will now be examined in greater detail.

It must first be determined if an attempted attack was successful. If the attack was successful, then there is a large amount of information to be gathered regarding the attack. If the attack was not successful, then learning about the type of attack may help evaluate future attacks. This is done by acquiring the same information as if the attack had been successful, except for determining what information was compromised. If it is unclear whether or not the attack was successful, it is better to follow the assumption that the attack was successful.

Once an intrusion has occurred, information about the intrusion must be collected. The first information required is to determine what has been compromised. This information will be used repeatedly in other areas.

Next, it must be determined what type of attack has occurred. A manager should acquire information in the following areas:

1. If the attack involved the interception of information:
   a. What information has been intercepted?
   b. Who does this information affect?
   c. How important is it that this person obtained access to this information?
2. If the attack involved the interruption of information:
   a. What information has been interrupted?
   b. Who/what does this interruption affect?
   c. Can the information be replaced?
   d. How important is this loss of information?
3. If the attack involved the modification of information:
   a. What information has been modified?
   b. Can this information be repaired or replaced?

c. How important is this modification of information?

4. If the attack involved the fabrication of information:

    a. What information has been fabricated?

    b. Who/what may have been affected by this fabricated information?

    c. How important is the existence of this fabricated information?

After this, a manager should analyze how the attack was accomplished. A manager should acquire information in the following areas:

1. For every attack on a stand-alone system:

    a. The method of attack used.

    b. If the attack used emissions:

        (1) Shielding of the system.

    c. If the attack used physical access:

        (1) Organization's security practices.

2. For every attack on a Intranet/LAN:

    a. The method of attack used.

    b. If the attack used physical access:

        (1) Organization's security practices.

    c. If the attack used emissions:

        (1) Shielding of nodes and links.

        (2) Encryption of messages and type of encryption.

3. For every attack on a system connected to the Internet:

    a. The method of attack used.

    b. If a message was intercepted external to the organization:

        (1) Encryption of messages and type of encryption.

    c. If attack occurred through the firewall:

        (1) Strengths and weaknesses of the your firewall.

Following this, a manager should know information regarding possible prosecution of the attackers. A manager should acquire information in the following areas:

1. Is a banner shown at log-in:
   a. Indicating entry is limited to authorized personnel, and that it is illegal for others to gain access to the system.
   b. The users actions may be monitored.
2. Has the attacker represented himself as someone else, such as logging in using someone else's password?
3. Is there a log tracing the actions of the attacker?

Finally, a manager should know information about how future attacks may be prevented. A manager should acquire information in the following areas:

1. Possible realignment of current assets used to secure the system.
2. Are additional assets required and available?

When all of this information has been captured, then a manager of an Air Force system will be able to make an informed decision regarding unauthorized computer entry.

Figure 11 embodies the entire process that a manager will follow to determine the information to be captured regarding unauthorized computer entry.

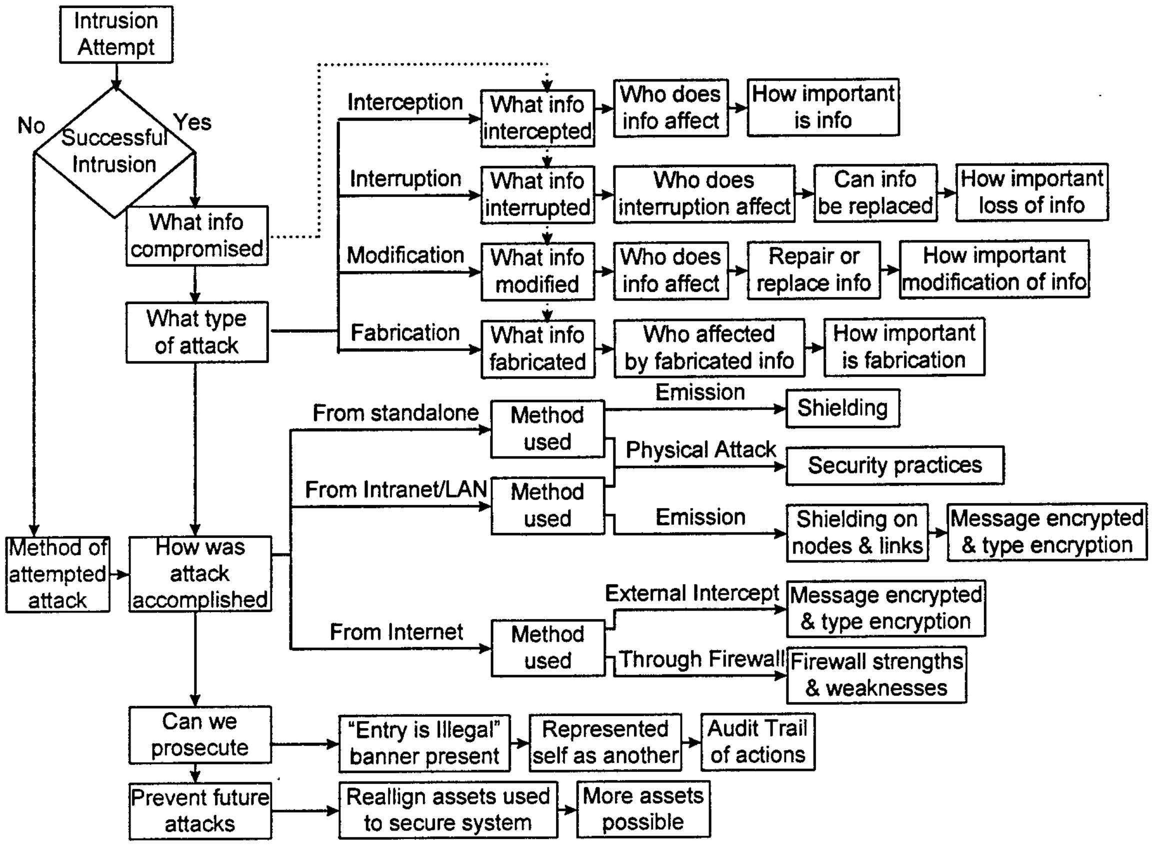

Figure 11. Initial Model for Determining Information to be Captured Regarding Unauthorized Computer Entry

Appendix E. Second Electronic Mail Message to Delphi Participants

Subject: Thesis Research

To: "AFCERT" <afcert@afcert.csap.af.mil>,
"ANS" <anscert@ans.net>,
"Apple Computer" <first-team@apple.com>,
"ASSIST" <assist@assist.mil>,
"Boeing CERT (BCERT)" <compsec@pss.boeing.com>,
"CERT" <cert@cert.org>,
"CIAC" <ciac@llnl.gov>,
"Cisco Systems" <first-team@cisco.com>,
"Digital Equipment Corporation SSRT"
<rich.boren@cxo.mts.dec.com>,
"EDS" <jim.cutler@iscg.eds.com>,
"General Electric Company" <Sandstrom@geis.geis.com>,
"Goldman, Sachs and Company" <shabbir.safdar@gs.com>,
"Hewlett-Packard Company" <security-alert@hp.com>,
"IBM-ERS" <ers@vnet.ibm.com>,
"MCI" <3557428@mcimail.com>,
"Motorola Comp. Emergency Resp. Team" <mcert@mot.com>,
"NASA Ames Research Center (Principle Center for Information Technology Security)" <ais@ames.arc.nasa.gov>,
"NASIRC" <Nasirc@nasirc.nasa.gov>,
"NAVCIRT" <jalucas@fiwc.navy.mil>,
"NIH CERT" <Kevin_Haney@nih.gov>,
"NIST/CSRC" <first-team@csmes.ncsl.nist.gov>,
"NU-CERT" <r-safin@nwu.edu>,
"OSU-IRT" <security@net.ohio-state.edu>,
"PCERT" <spaf@cs.purdue.edu>,
"REACT-SAIC" <paz@cip.saic.com>,
"SBACERT" <hfbolden@sba.gov>,
"SGI" <mccauley@phaeton.engr.sgi.com>,
"Sprint" <mike@sprint.net>,
"SSACERT" <ssacert@ssa.gov>,
"SUN Microsystems" <chok@barrios.eng.sun.com>,
"SUNSeT" <security@stanford.edu>,
"TRW Inc" <zorn@gumby.sp.trw.com>,
"UCERT" <garygarb@unn.unisys.com>,
"USHCERT" <security@mail.house.gov>,
"US Veterans Health Administration"
<frank.marino@forum.va.gov>

cc: "Dr. Heminger" <aheminge@afit.af.mil>,
"Maj. Vickery" <cvickery@afit.af.mil>

Dear Sir or Ma'am,

Thank you very much for your comments and suggestions on my thesis model, "Determining Information to be Captured Regarding Unauthorized Computer Entry." They proved

extremely insightful in highlighting deficiencies in the model as well as suggesting more emphasis in particular areas.

I have attempted to incorporate your improvements into my improved model. I would be very appreciative if you would review my improved model and make any further comments on how this improved model may be further improved.

If possible, please return your comments by October 24th. I will then consolidate the comments and create a further improved model. If there are significant improvements, I will then send this further improved model out for your assessment. Again, in all further improved models and my final thesis, no comments will be attributed to particular individuals or organizations.

The improved model is attached as model.doc in Microsoft Word 7.0 or as model.txt in ASCII Text, without the two figures

I may be reached at 937-255-7777x2131, (DSN prefix 785 for military units), or <lhimebro@afit.af.mil>. My thesis advisor and program manager for Information Resource Management is Dr. Alan Heminger, who may be reached at 937-255-1210, or <aheminge@afit.af.mil>.

A completed copy of my thesis will be sent to you by electronic mail (zipped as Microsoft Word 7.0) if you requested a copy. I am due to graduate on December 16th, and hope that I will be sending my final thesis during the beginning half of December.

Again, thank you very much for your assistance.

LESLIE F. HIMEBROOK, 1Lt, USAF
Graduate Student, Air Force Institute of Technology

The model that was attached to this electronic mail message is located in Appendix F. Second Model Sent to Delphi Participants on page 60.

Appendix F. Second Model Sent to Delphi Participants

In order for an Air Force manager to be able to make decisions regarding unauthorized computer entry, certain information must be captured. The areas in which a manager must have information are summarized in the model shown in Figure 12.

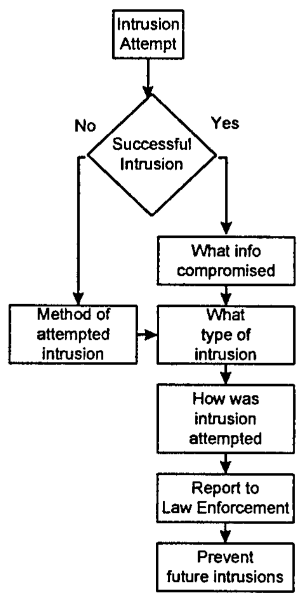

Figure 12. Overview Model After First Round of Delphi for Determining Information to be Captured Regarding Unauthorized Computer Entry

Intrusion Attempt

An intrusion attempt is defined as an act which is intentionally employed for the purpose of gaining unauthorized access to a computer or computer system. Once an intrusion has been attempted, it must be decided whether the intrusion was successful. A successful intrusion is defined as an act which is intentionally employed for the purpose of and is successful at gaining unauthorized access to a computer or computer system. If it was unsuccessful, noting the type of intrusion in a database may by useful for future analysis and comparison with other organizations. If the intrusion was successful, then

information must be gathered in several additional areas. This would include the type of intrusion and what information was compromised, the method of the intrusion, whether the intruders should be reported to law enforcement authorities, and what may be done to prevent future intrusions. With this information, a manager will be able to make an informed decision regarding the unauthorized computer entry. Each of these areas will now be examined in greater detail.

Successful Intrusion Determination

It must first be determined if there was an intrusion, and whether or not it was successful. If the intrusion was successful, then there is additional information to be gathered regarding the intrusion. If the intrusion was not successful, then learning about the type of intrusion may help evaluate future intrusions. If it is unclear whether or not the intrusion was successful, it is better to follow the assumption that the intrusion was successful.

If the intrusion was successful, it is important to determine what has been compromised. This information will be used repeatedly in other areas, such as the type of attack.

What Information was Compromised and What Type of Intrusion

It must be determined what type of intrusion has occurred. A manager should acquire information in the following areas:

1. If the intrusion involved the interception of information:
    a. What information has been intercepted?
    b. Who does this information affect?
    c. How important is it that this person obtained access to this information?
2. If the intrusion involved the interruption or denial of information:
    a. What information has been interrupted?
    b. Who/what does this interruption affect?

c. Can the information be replaced?

d. How important is this loss of information?

3. If the intrusion involved the modification of information:

   a. What information has been modified?

   b. Can this information be repaired or replaced?

   c. How important is this modification of information?

4. If the intrusion involved the fabrication of information:

   a. What information has been fabricated?

   b. Who/what may have been affected by this fabricated information?

   c. How important is the existence of this fabricated information?

5. If the intrusion did not attempt to interrupt, intercept, modify, or fabricate any information:

   a. Was the system probed only to determine if intrusion is possible?

How the Intrusion was Attempted

A manager should analyze how the intrusion was accomplished. A manager should acquire information in the following areas:

1. For every intrusion on a stand-alone system, what method of intrusion was used?

   a. If the intrusion used emissions:

      (1) Has shielding to prevent emissions been placed around the system to prevent intrusion?

      (2) Is the system shielded to prevent emissions due to its location in the building?

   b. If the intrusion used physical access:

      (1) What are the organization's security practices?

      (2) What are the organization's policies regarding computer security?

2. For every intrusion on a Intranet/LAN, what method of intrusion was used?
    a. If the intrusion used physical access:
        (1) What are the organization's security practices?
        (2) What are the organization's policies regarding computer security?
    b. If the intrusion used emissions:
        (1) Has shielding to prevent emissions been placed around the system to prevent intrusions?
        (2) Is the system shielded to prevent emissions due to the location in or between buildings?
        (3) Was encryption of messages used and what type of encryption?
3. For every intrusion of a system connected to the Internet, what method of intrusion was used?
    a. If a message was intercepted external to the organization:
        (1) Was encryption of messages used and what type of encryption?
    b. If intrusion occurred through the firewall:
        (1) What are the strengths and weaknesses of the your firewall?
        (2) Was a Guest Login used through the firewall?
4. For every intrusion of a system through a modem:
    a. What are the organization's security practices?
    b. What are the organization's policies regarding computer security?
    c. Was a Guest Login used?

Report to Law Enforcement

A manager should know information regarding reporting of intruders to Law Enforcement. A manager should acquire information in the following areas:

1. Is a banner shown at log-in on the port that was used?

a. Does the banner indicate that entry is limited to authorized personnel, and that it is illegal for others to gain access to the system?

b. Does the banner indicate that the user's actions may be monitored?

2. Has the intruder represented himself as someone else, such as logging in using someone else's password?
3. Is there a log tracing the actions of the intruder?
4. Has the appropriate CERT been notified of the intrusion attempt?

Preventing Future Intrusions

A manager should know information about how future intrusions may be prevented. A manager should acquire information in the following areas:

1. Have all published security patches for known security deficiencies been installed?
2. Are necessary manpower, money and systems available to the system administrator to secure the system?
3. Are additional manpower, money and systems available to secure the system?

Conclusion

When all of this information has been captured, then a manager of an Air Force system will be able to make an informed decision regarding unauthorized computer entry.

Figure 13 embodies the entire process that a manager will follow to determine the information to be captured regarding unauthorized computer entry.

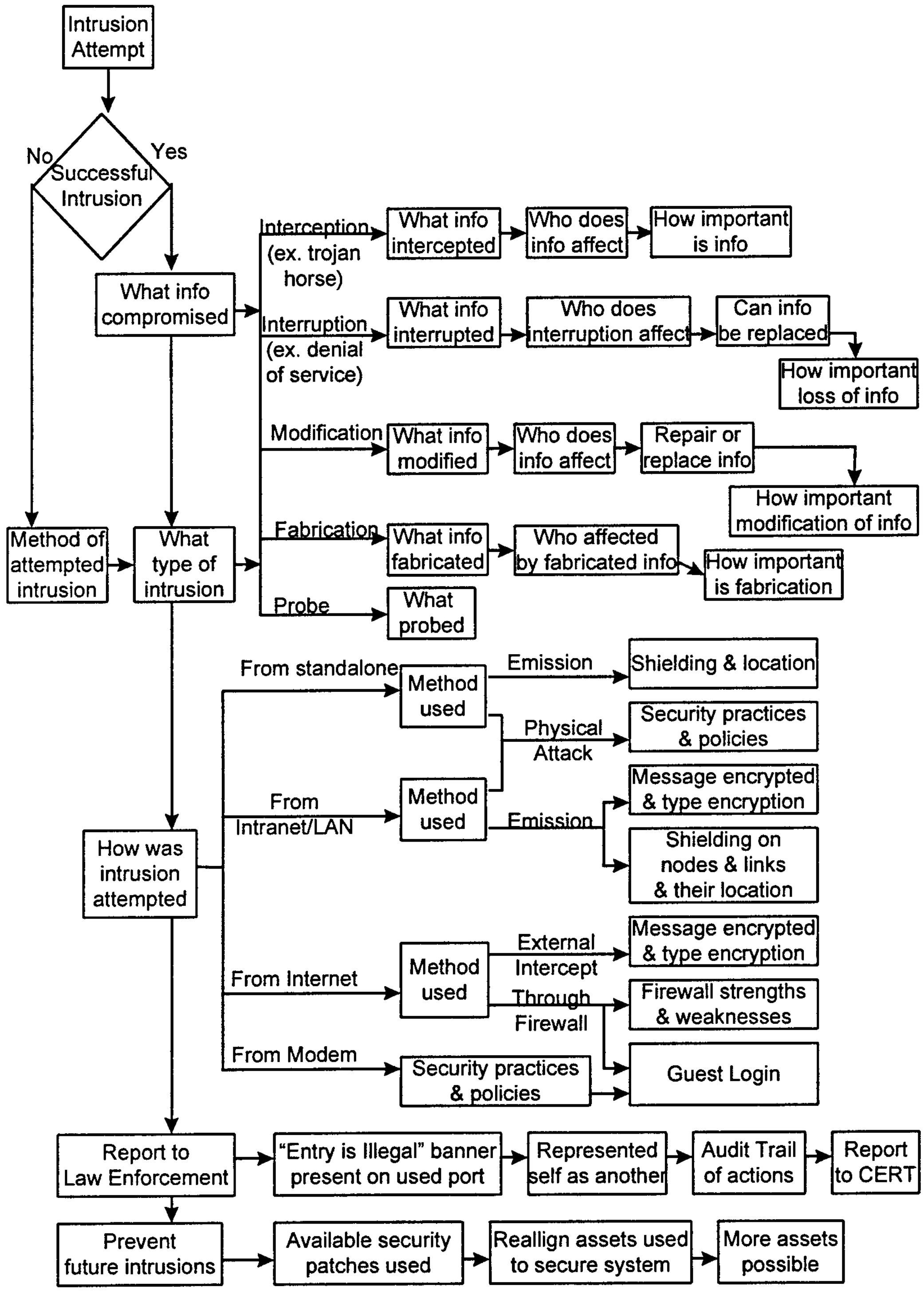

Figure 13. Model After First Round of Delphi for Determining Information to be Captured Regarding Unauthorized Computer Entry

Appendix G. Final Model

In order for an Air Force manager to be able to make decisions regarding unauthorized computer entry, certain information must be captured. The areas in which a manager must have information are summarized in the model shown in Figure 14.

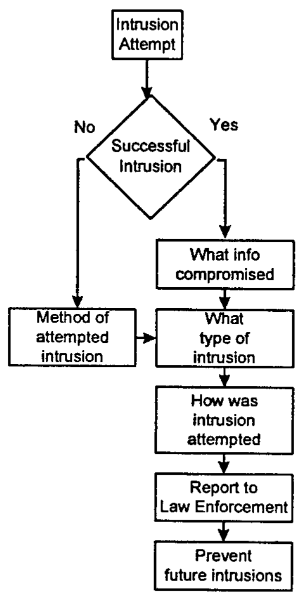

Figure 14. Final Overview Model for Determining Information to be Captured Regarding Unauthorized Computer Entry

Intrusion Attempt

An intrusion attempt is defined as an act which is intentionally employed for the purpose of gaining unauthorized access to a computer or computer system. Once an intrusion has been attempted, it must be decided whether the intrusion was successful. A successful intrusion is defined as an act which is intentionally employed for the purpose of and is successful at gaining unauthorized access to a computer or computer system. If it was unsuccessful, noting the type of intrusion in a database may by useful for future analysis and comparison with other organizations. If the intrusion was successful, then

information must be gathered in several additional areas. This would include the type of intrusion and what information was compromised (losses), the method of the intrusion (threats), whether the intruders should be reported to law enforcement authorities (policies), and what may be done to prevent future intrusions (costs). With this information, a manager will be able to make an informed decision regarding the unauthorized computer entry. The order that the information should be gathered in will vary, depending on the situation. The order that it is presented in is a probable order in which the information would be gathered. Each of these areas will now be examined in greater detail.

Successful Intrusion Determination

It must first be determined if there was an intrusion, and whether or not it was successful. For successful intrusions there is much additional information to be gathered regarding the intrusion. On unsuccessful intrusions, knowledge about the type of intrusion may help evaluate future intrusions. If it is unclear whether or not the intrusion was successful, it is better to follow the assumption that the intrusion was successful.

If the intrusion was successful, it is important to determine what has been compromised. This information will be used repeatedly in other areas, such as the type of attack.

What Information was Compromised and What Type of Intrusion

It must be determined what type of intrusion has occurred. A manager should acquire information in the following areas:

1. If the intrusion involved the interception of information:
    a. What information has been intercepted?
    b. Who does this information affect?
    c. How important is it that this person obtained access to this information?
2. If the intrusion involved the interruption or denial of information:

a. What information has been interrupted?

b. Who/what does this interruption affect?

c. Can the information be replaced?

d. How important is this loss of information?

3. If the intrusion involved the modification of information:

   a. What information has been modified?

   b. Can this information be repaired or replaced?

   c. How important is this modification of information?

4. If the intrusion involved the fabrication of information:

   a. What information has been fabricated?

   b. Who/what may have been affected by this fabricated information?

   c. How important is the existence of this fabricated information?

5. If the intrusion did not attempt to interrupt, intercept, modify, or fabricate any information:

   a. Was the system probed only to determine if intrusion is possible?

How the Intrusion was Attempted

A manager should analyze how the intrusion was accomplished. A manager should acquire information in the following areas:

1. For every intrusion on a stand-alone system, what method of intrusion was used?

   a. If the intrusion used emissions:

      (1) Has shielding to prevent emissions been placed around the system to prevent intrusion?

      (2) Is the system shielded to prevent emissions due to its location in the building?

   b. If the intrusion used physical access:

(1) What are the organization's security practices?

(2) What are the organization's policies regarding computer security?

2. For every intrusion on a Intranet/LAN, what method of intrusion was used?

   a. If the intrusion used physical access:

      (1) What are the organization's security practices?

      (2) What are the organization's policies regarding computer security?

   b. If the intrusion used emissions:

      (1) Has shielding to prevent emissions been placed around the system to prevent intrusions?

      (2) Is the system shielded to prevent emissions due to the location in or between buildings?

      (3) Was encryption of messages used and what type of encryption?

3. For every intrusion of a system connected to the Internet, what method of intrusion was used?

   a. If a message was intercepted external to the organization:

      (1) Was encryption of messages used and what type of encryption?

   b. If intrusion occurred through the firewall:

      (1) What are the strengths and weaknesses of the your firewall?

      (2) Was a Guest Login used through the firewall?

4. For every intrusion of a system through a modem:

   a. What are the organization's security practices?

   b. What are the organization's policies regarding computer security?

   c. Was a Guest Login used?

Report to Law Enforcement

A manager should know information regarding reporting of intruders to Law Enforcement. A manager should acquire information in the following areas:

1. Is a banner shown at log-in on the port that was used?
    a. Does the banner indicate that entry is limited to authorized personnel, and that it is illegal for others to gain access to the system?
    b. Does the banner state that the user's actions may be monitored?
2. Has the intruder represented himself as someone else, such as logging in by using someone else's password?
3. Is there a log which traces the actions of the intruder?
4. Has the appropriate CERT been notified of the intrusion attempt?

Preventing Future Intrusions

A manager should know information about how future intrusions may be prevented. A manager should acquire information in the following areas:

1. Have all published security patches for known security deficiencies been installed?
2. Are necessary manpower, money and systems available to the system administrator to secure the system?
3. Are additional manpower, money and systems available to secure the system?

Conclusion

When all of this information has been captured, then a manager of an Air Force system will be able to make an informed decision regarding unauthorized computer entry.

Figure 15 embodies the entire process that a manager will follow to determine the information to be captured regarding unauthorized computer entry.

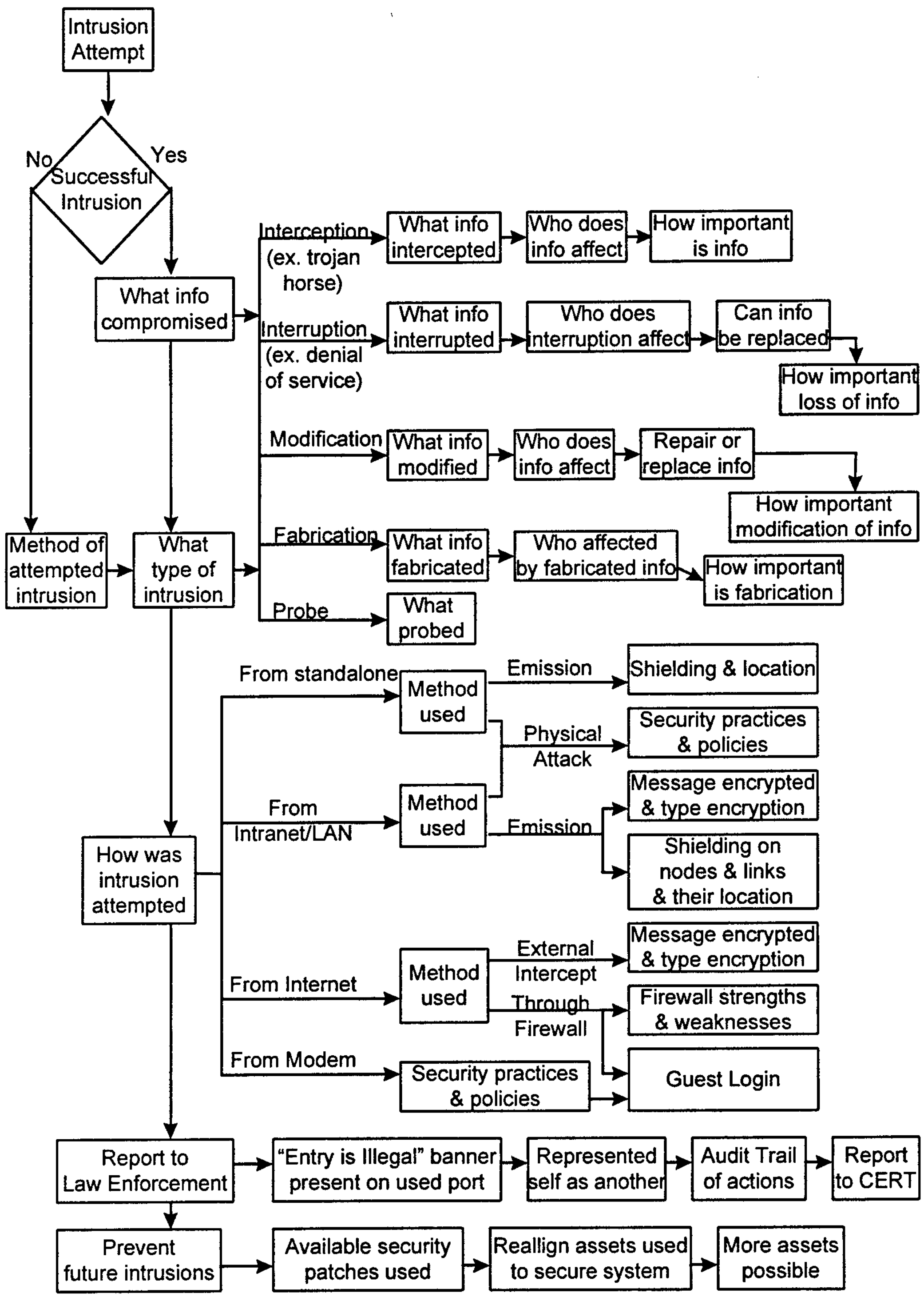

Figure 15. Final Model for Determining Information to be Captured Regarding Unauthorized Computer Entry

References

Anthens, Gary H. "Security Pundits Weigh War Threat," Computerworld: 80 (October 2, 1995).

Arquilla, John. "The Strategic Implications of Information Dominance," Strategic Review: 24-30 (Summer 1994).

Braaten, J. and J. T. Johannessen. "Security in Defense Communications Systems," Electrical Communications, 65 # 3: 263-269 (1992).

Brown, Bernice B. Delphi Process: A Methodology Used for the Elicitation of Opinions of Experts. Report Series P-3925. Santa Monica: The RAND Corporation, 1968.

Brown, Bernice B. and Olaf Helmer. Improving the Reliability of Estimates Obtained From a Consensus of Experts. Report Series P-2986. Santa Monica: The RAND Corporation, 1964.

Busey, James B. IV. "Information Warfare Calculus Mandates Protective Actions," Signal: 15 (October, 1994).

Connolly, Julie L. "Operation Chain Link: The Deployment of a Firewall at Hanscom Air Force Base," Proceedings of the 12th Annual Computer Security Applications Conference. 170-177. Los Alamitos CA: IEEE Computer Society Press, 1996.

Creasy, Sir Edward S. Fifteen Decisive Battles of the World (Second Edition). Harrisburg: The Stackpole Company, 1955.

Dalkey, Norman C. Delphi. Report Series P-3704. Santa Monica: The RAND Corporation, 1967.

Dalkey, Norman C. The Delphi Method: An Experimental Study of Group Opinion. Report Series RM-5888-PR. Santa Monica: The RAND Corporation, 1969.

Executive Order 12958. Classified National Security Information. Washington: Government Printing Office, April 17, 1995.

FIRST. "FIRST Team Contact Information." WWWeb, http://www.first.org/team-info/ (16 Aug 97).

FIRST. "What is FIRST?" WWWeb, http://www.first.org/about/ (16 Aug 97).

Fithen, Katherine and Barbara Fraser. "CERT Incident Response and the Internet," Communications of the ACM, 37: 108-113 (August 1994).

Fogleman, Ronald D. "What Information Warfare Means To You," Air Force Times, 55: 31 (Jul 17, 1995).

Government Accounting Office/Accounting and Information Management Division. Defense Information Security. Report Series GAO/AIMD-96-84. Washington: Government Printing Office, 1996.

Harvey, Christopher. "CERT—Computer Emergency Response Team," Computer Networks and ISDN Systems, 23: 167-170 (November 1991).

Hastings, Max. Overlord, D-Day and the Battle for Normandy. New York: Simon and Schuster, 1968.

Heflin, Woodford A., ed. The United States Air Force Dictionary. Air University Press, 1956.

Howard, John D. An Analysis of Security Incidents on the Internet: 1989-1995. Ph.D. dissertation. Carnegie Mellon University, Pittsburgh PA, 1997.

Johnson John T. and Kevin Tolly. "The Safety Catch: Token Authentication," Data Communications: 62-77 (May 1995).

Koch, James R. "Operation Fortitude, the Backbone of Deception," Military Review: 66-77 (March 1992).

Luo, Dongxin and Jack L. Armitage. "A Risk Analysis Approach to Control and Audit in a Network Environment," Internal Auditing: 13-22 (Fall 1996).

Minihan, Kenneth A. "Information Dominance: Meeting the Intelligence Needs of the 21st Century," Air Intelligence Journal, 15: 15-19 (Spring/Summer 1994).

Muldoon, William C. Jr. Area Defense Council, Wright-Patterson AFB OH. Personal Interview. 11 Sep 1997.

Office of Management and the Budget. Management of Federal Information Resources. OMB Circular No. A-130. Washington: Government Printing Office, February 8, 1996.

Rackoff, Charles and Daniel R. Simon. "Cryptographic Defense Against Traffic Analysis," Proceedings of the 25th Annual Symposium on the Theory of Computing. 672-681. New York: ACM Press, 1993.

Rona, Thomas P. "Information Warfare: An Age-old Concept With New Sights," Defense Intelligence Journal, 5: 53-67 (Spring 1996).

Schwartau, Winn. Information Warfare (Second Edition). New York: Thunder's Mouth Press, 1996.

Snow, D. and W. Chang. "Network Security," NTC-92. National Telesystems Conference. 15/13-16. New York: IEEE press, 1992.

Soma, John T. and others. Legal Guide to Computer Crime: A Primer for Investigators and Judge Advocates. Prepared by the Office of the Staff Judge Advocate, Air Force Office of Special Investigations, Bolling AFB DC. no date [1994].

Sun Tzu. The Art of War. Trans. Samuel B. Griffith. New York: Oxford University Press, 1963.

Surlowitz, David L. "Information Protection, Concept of Operations." Briefing with slides. Air Force Computer Emergency Response Team, Kelly AFB TX 27 December 1996.

Szafarsnski, Richard. "A Theory of Information Warfare: Preparing for 2020," Airpower Journal: 56-65 (Spring 1995).

Thatcher, Byron B. Operations Officer, Air Force Computer Emergency Response Team, Air Intelligence Agency, Kelly AFB TX. Personal Interview. 26 Mar 1997.

Thrasher, Roger D. "Information Warfare Delphi: Characteristics of Information Warfare." Information Warfare (Second Edition). Ed. Winn Schwartau. New York: Thunder's Mouth Press, 1996. 579-587.

Van Eck, William. "Electromagnetic Radiation From Video Display Units: An Eavesdropping Risk?," Computers & Security, 4: 269-286 (1985).

Vita

Lieutenant Leslie F. Himebrook is from Zavalla County, Texas. He graduated from the Air Force Academy in 1994 with a Bachelor of Science degree in Space Operations. After receiving his commission, Lieutenant Himebrook was assigned as the Squadron Adjutant to the 52nd Flying Training Squadron (FTS) at Reese AFB, Texas.

With the drawdown of Reese AFB, Lieutenant Himebrook entered the Air Force Institute of Technology at Wright-Patterson AFB, Ohio, and graduated in 1997 with a Masters degree in Information Systems Management. He was subsequently assigned to the Air Force Operational Test And Evaluation Center, Kirtland AFB, New Mexico.

Permanent Address: 602 Sunglow Ave.
Alamogordo NM 88310-4131

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1997	Master's Thesis

4. TITLE AND SUBTITLE
A MODEL FOR DETERMINING INFORMATION TO BE CAPTURED REGARDING UNAUTHORIZED COMPUTER ENTRY OF AN AIR FORCE COMPUTER SYSTEM

5. FUNDING NUMBERS

6. AUTHOR(S)
Leslie F. Himebrook, 1Lt, USAF

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
2750 P Street
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIS/LAS/97D-1

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFIWC/EACA
102 Hall Blvd, Ste 215
KAFB TX 78243-7013

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 Words*)

This thesis presents a model of information to capture regarding unauthorized computer systems access attempts. This model takes a management focus, and incorporates the technical focus, intelligence focus, and legal focus as inputs. The author used an exploratory, qualitative methodology consisting of an extensive literature review and interviews with experts in the field. These efforts produced the proposed model, which was reviewed by experts in the field using a delphi technique.

The model consists of information that is divided into the following areas: 1. What information was compromised. 2. What type of intrusion occurred. 3. How the intrusion was attempted. 4. Ability to report to law enforcement. 5. Prevention of future intrusions.

This thesis concludes by recommending: 1. Information should be captured by individual as close to the intrusion as possible. This is to reduce inaccuracies in the information. 2. Information should be passed in a timely and accurate manner to the organization's CERT. 3. The CERT should use the information to rectify the intrusion. 4. The CERT should conglomerate the information to evaluate the possibility of an organized intrusion attempt. 5. The CERT should pass relevant information to other system administrators to prevent future successful intrusion attempts.

14. SUBJECT TERMS

Network Security, Computer Security, Information Security

15. NUMBER OF PAGES
87

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

AFIT Control Number AFIT/GIS/LAS/97D-1

AFIT RESEARCH ASSESSMENT

The purpose of this questionnaire is to determine the potential for current and future applications of AFIT thesis research. **Please return completed questionnaire** to: AIR FORCE INSTITUTE OF TECHNOLOGY/LAC, 2950 P STREET, WRIGHT-PATTERSON AFB OH 45433-7765. Your response is **important.** Thank you.

1. Did this research contribute to a current research project? a. Yes b. No

2. Do you believe this research topic is significant enough that it would have been researched (or contracted) by your organization or another agency if AFIT had not researched it?
a. Yes b. No

3. **Please estimate** what this research would have cost in terms of manpower and dollars if it had been accomplished under contract or if it had been done in-house.

Man Years____________ $____________

4. Whether or not you were able to establish an equivalent value for this research (in Question 3), what is your estimate of its significance?

a. Highly Significant b. Significant c. Slightly Significant d. Of No Significance

5. Comments (Please feel free to use a separate sheet for more detailed answers and include it with this form):

____
Name and Grade

____
Organization

____
Position or Title

____
Address